

# vSphere の可用性

Update 1

変更日：2020 年 8 月 13 日

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**ヴィエムウェア株式会社**  
〒108-0023 東京都港区芝浦 3-1-1  
田町ステーションタワー N 18 階  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2009-2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

vSphere の可用性について 5

更新情報 6

## 1 ビジネス継続性とダウンタイムの最小化 7

計画的ダウンタイムの短縮 7

計画外のダウンタイムの防止 8

vSphere HA が提供する、システム停止からの迅速なリカバリ 8

vSphere Fault Tolerance が提供する継続的な可用性 9

## 2 vSphere HA クラスタの作成と使用 11

vSphere HA の動作 11

プライマリ ホストとセカンダリ ホスト 12

ホスト障害のタイプと検出 12

ホスト問題に対する対応の決定 13

仮想マシンとアプリケーションの監視 17

仮想マシン コンポーネント保護 18

ネットワーク パーティション 19

データストア ハートビート 20

vSphere HA セキュリティ 20

vSphere HA のアドミッション コントロール 21

クラスタで許容するホスト障害アドミッション コントロール ポリシー 22

予約されたクラスタ リソースの割合アドミッション コントロール ポリシー 25

フェイルオーバー ホストの指定アドミッション コントロール ポリシー 27

アドミッション コントロール ポリシーの選択 28

vSphere HA の相互運用性 29

vSphere HA と Virtual SAN の併用 29

vSphere HA と DRS の併用 30

vSphere HA の相互運用性に関するその他の問題 32

vSphere HA クラスタの作成および構成 33

vSphere HA のチェックリスト 33

vSphere HA クラスタの作成 34

vSphere HA クラスタ設定の構成 36

vSphere HA クラスタのベスト プラクティス 42

ネットワークのベスト プラクティス 42

相互運用性のベスト プラクティス 44

アドミッション コントロールのベスト プラクティス 45

クラスタ監視のベスト プラクティス 46

### 3 仮想マシンの Fault Tolerance の準備 47

Fault Tolerance の機能 47

Fault Tolerance の使用事例 48

Fault Tolerance の要件、制限、およびライセンス 49

Fault Tolerance の相互運用性 50

Fault Tolerance でサポートされない vSphere の機能 50

Fault Tolerance と互換性のない機能とデバイス 50

Fault Tolerance と DRS の併用 51

Fault Tolerance に向けたクラスタとホストの準備 52

Fault Tolerance のチェックリスト 52

ホスト マシンのネットワークの構成 54

クラスタの作成とコンプライアンスのチェック 55

フォールトトレランスの使用 55

Fault Tolerance をオンにするときの検証 55

Fault Tolerance をオン 56

Fault Tolerance をオフ 57

Fault Tolerance のサスペンド 58

セカンダリの移行 58

フェイルオーバーのテスト 58

セカンダリの再起動テスト 59

Fault Tolerance で使用するホストのアップグレード 59

Fault Tolerance のベスト プラクティス 60

レガシー Fault Tolerance 62

レガシー Fault Tolerance の有効化 64

# vSphere の可用性について

『vSphere Availability』は、vSphere<sup>®</sup> High Availability (HA) と vSphere フォールトトレランスの設定方法など、ビジネスに継続性を与えるソリューションについて説明します。

## 対象読者

この情報は、vSphere HA およびフォールトトレランスのソリューションを使用してビジネスに継続性を与える立場の方を対象としています。本書の情報は、仮想マシンテクノロジーおよびデータセンター運用に精通した、経験の豊富な Windows または Linux システムの管理者向けです。

# 更新情報

この『vSphere の可用性』は、製品のリリースごとに、または必要に応じて更新されます。

『vSphere の可用性』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2020 年 8 月 10 日	VMware では、多様性の受け入れを尊重しています。弊社のお客様、パートナー、内部コミュニティにおいてこの原則を推進するため、弊社のコンテンツに含まれている用語の見直しを行っています。不適切な表現を削除するため、このガイドを更新しました。
2016 年 10 月 07 日	初期リリース。

# ビジネス継続性とダウンタイムの最小化

# 1

計画的または計画外のいずれの場合でも、ダウンタイムによって多大なコストが生じます。一方、従来、高いレベルの可用性を実現するためのソリューションはコストがかかり、実装が複雑で、管理が困難でした。

当社のソフトウェアを使用すると、より簡単で安価に、重要なアプリケーションに対する高いレベルの可用性を実現できます。vSphere を使用すると、組織はより簡単で安価に、高いレベルの可用性を実現できるだけでなく、すべてのアプリケーションに対して提供される可用性の基準レベルを向上させることができます。vSphere を使用すると、ユーザーは次のことが可能になります。

- ハードウェア、オペレーティング システム、およびアプリケーションとは関係なく、高可用性を実現できます。
- 一般的なメンテナンス操作のための計画的ダウンタイムを減らすことができます。
- 障害が発生した場合に、自動的にリカバリできます。

vSphere では、計画的なダウンタイムを減らす、計画外のダウンタイムを回避する、停止状態から迅速に回復するなどが可能です。

この章には、次のトピックが含まれています。

- [計画的ダウンタイムの短縮](#)
- [計画外のダウンタイムの防止](#)
- [vSphere HA が提供する、システム停止からの迅速なリカバリ](#)
- [vSphere Fault Tolerance が提供する継続的な可用性](#)

## 計画的ダウンタイムの短縮

計画的ダウンタイムは一般に、データセンターのダウンタイムの 80% 以上を占めます。ハードウェアのメンテナンス、サーバの移行、ファームウェアの更新はすべて、物理サーバのダウンタイムを必要とします。このダウンタイムの影響を最小限にするために、組織は、不便でスケジュール設定が困難なダウンタイム用時間枠までメンテナンスを遅らせざるをえません。

vSphere では、組織は計画的ダウンタイムを大幅に短縮できます。vSphere 環境では、ダウンタイムやサービスの中断なしにワークロードを動的に別の物理サーバに移動できるため、アプリケーションとサービスのダウンタイムを必要とせずにサーバのメンテナンスを実行できます。vSphere を使用すると、組織は次のことができます。

- 一般的なメンテナンス操作のためのダウンタイムを排除できます。
- 計画的なメンテナンス用時間枠をなくすことができます。

- ユーザーの操作やサービスを中断せずに、いつでもメンテナンスを行うことができます。

vSphere における vSphere vMotion<sup>®</sup> 機能と Storage vMotion 機能により、組織は計画的ダウンタイムを短縮できます。VMware 環境ではサービスの中断なしに、ワークロードを別の物理サーバまたは別の基盤ストレージへ動的に移動できるからです。システム管理者は、不便なメンテナンス用時間枠のスケジュール設定を強制されずに、迅速かつ完全に透過的なメンテナンス操作を実行できます。

## 計画外のダウンタイムの防止

実行中のアプリケーションに対して ESXi ホストが堅牢なプラットフォームを提供する一方で、組織も、ハードウェアやアプリケーションの障害により生じる計画外のダウンタイムから自分自身を守る必要があります。vSphere は、ユーザーが計画外のダウンタイムを防止する際に役立つ重要な機能を、データセンターのインフラストラクチャに組み込みます。

これらの vSphere の機能は仮想インフラストラクチャの一部であり、仮想マシン上で動作するオペレーティングシステムやアプリケーションに対して透過的です。これらの機能は構成可能で、物理システム上のすべての仮想マシンで利用されるため、高可用性を提供する際のコストと複雑さが軽減されます。vSphere に組み込まれている可用性の主要な機能は、次のとおりです。

- 共有ストレージ。ファイバ チャネル SAN や iSCSI SAN、または NAS などの共有ストレージに仮想マシンのファイルを格納することで、単一点障害を除去します。SAN のミラーリングおよびレプリケーション機能を使用して、ディザスタ リカバリ サイトで仮想ディスクの更新コピーを維持できます。
- ネットワーク インターフェイス チェミング。個々のネットワーク カード障害に対応します。
- ストレージのマルチパス機能。ストレージのパス障害に対応します。

これらの機能に加え、vSphere HA 機能とフォールト トレランス機能は、システム停止からの迅速なリカバリと継続的な可用性をそれぞれが提供することで、計画外のダウンタイムを最小限にするか、排除することができます。

## vSphere HA が提供する、システム停止からの迅速なリカバリ

vSphere HA は、クラスタとして構成されている複数の ESXi ホストを活用して、仮想マシンで実行中のアプリケーションに、システム停止からの迅速なリカバリと、費用対効果に優れた高可用性を提供します。

vSphere HA は、次の方法でアプリケーションの可用性が向上します。

- サーバ障害に対しては、仮想マシンをクラスタ内のほかのホストで再起動することで向上します。
- ゲスト OS 障害によるアプリケーション障害に対しては、仮想マシンを継続的に監視し、障害が検出された際に仮想マシンをリセットすることで向上します。
- まだデータストアにアクセスできる他のホストで、影響を受けている仮想マシンを再起動して、データストアのアクセシビリティ障害から保護します。
- 管理ネットワークまたは Virtual SAN ネットワークでホストが隔離されると、再起動することによって仮想マシンをネットワーク隔離から保護します。この保護は、ネットワークがパーティション分割されている場合でも行われます。



ほかのクラスタリング ソリューションとは異なり、vSphere HA はインフラストラクチャを提供して、全ワークロードをそれにより保護できるようにします。

- アプリケーションまたは仮想マシンに特別なソフトウェアをインストールする必要はありません。vSphere HA が全ワークロードを保護するからです。vSphere HA を構成したあとは、新しい仮想マシンを保護するための操作は不要です。自動的に保護されます。
- vSphere HA を vSphere DRS (Distributed Resource Scheduler) と組み合わせると、障害に対する保護と、クラスタ内の複数のホストにわたるロード バランシング機能を提供できます。

vSphere HA には、従来のフェイルオーバー ソリューションと比べていくつかのメリットがあります。

### 最小限のセットアップ

vSphere HA クラスタのセットアップ後、追加の構成を行わずにクラスタ内のすべての仮想マシンがフェイルオーバーのサポートを受けます。

### ハードウェアのコストとセットアップの削減

仮想マシンは、移動可能なアプリケーション用コンテナとして機能し、ホスト間で移動できます。システム管理者は、複数のマシン上の重複する構成を回避できます。vSphere HA を使用する場合は、vSphere HA で保護したい数のホストをフェイルオーバーするのに十分なリソースがなければなりません。ただし、vCenter Server システムは自動的にリソースを管理し、クラスタを構成します。

### アプリケーションの可用性の向上

仮想マシン内で実行されるどのアプリケーションも、可用性が向上します。仮想マシンはハードウェア障害から復旧できるため、アプリケーション自体がクラスタリングされたアプリケーションでなくても、コンピューティング要件を加えることなく、ブート時に起動するすべてのアプリケーションの可用性が向上します。VMware Tools のハートビートを監視して応答し、応答しない仮想マシンを再起動することで、ゲスト OS のクラッシュから保護できます。

### DRS と vMotion の統合

ホストに障害が起き、仮想マシンがほかのホスト上で再起動された場合、DRS は、バランスのとれたリソース割り当てを行うために、移行の推奨を提供するか、仮想マシンを移行できます。移行元ホストと移行先ホストのいずれか一方または両方に障害が起きた場合、vSphere HA が障害からの復旧に役立ちます。

## vSphere Fault Tolerance が提供する継続的な可用性

vSphere HA は、ホスト障害時に仮想マシンを再起動することにより、仮想マシンに対して基本レベルの保護機能を提供します。vSphere フォールトトレランスは、より高度な可用性を提供します。ユーザーはデータ、トランザクション、または接続を失うことなくホスト障害から仮想マシンを保護できます。

フォールトトレランスは、仮想マシンの命令実行時のどの時点においても、プライマリおよびセカンダリ仮想マシンの状態を必ず同一にすることで継続的な可用性を実現します。

プライマリ仮想マシンを実行しているホスト、またはセカンダリ仮想マシンを実行しているホストのどちらかで障害が発生すると、直ちに透過的なフェイルオーバーが発生します。ネットワーク接続や処理中のトランザクションを失うことなく、正常機能している ESXi ホストがシームレスにプライマリ仮想マシンのホストになります。透過的なフェイルオーバーでは、データが失われず、ネットワーク接続が維持されます。透過的なフェイルオーバーの発生後は、新しいセカンダリ仮想マシンが再作成され、冗長性が再確立されます。プロセス全体は透過的で完全に自動的に行われ、vCenter Server が利用不可能な場合でも実行されます。

# vSphere HA クラスタの作成と使用

# 2

vSphere HA クラスタによって、ESXi ホストの集合が1つのグループとして機能するようになるため、ESXi ホストがそれぞれ個別に機能する場合に比べて、仮想マシンの高い可用性を実現できます。新しい vSphere HA クラスタの作成と使用を計画する場合、選択したオプションによって、ホストまたは仮想マシンの障害に対するクラスタの対処方法が異なります。

vSphere HA クラスタを作成する前に、vSphere HA がホスト障害を確認して切り分け、対処する方法を知る必要があります。また、アドミッション コントロールの動作を知り、フェイルオーバーに関する実際のニーズに適したポリシーを選択できるようにします。クラスタの作成後は、詳細オプションを使用して動作をカスタマイズし、推奨ベスト プラクティスに従ってパフォーマンスを最適化できます。

---

**注：** vSphere HA を使用しようとしたとき、エラー メッセージが出ることがあります。vSphere HA に関するエラー メッセージについては、次の VMware ナレッジ ベースを参照してください。<http://kb.vmware.com/kb/1033634>

---

この章には、次のトピックが含まれています。

- vSphere HA の動作
- vSphere HA のアドミッション コントロール
- vSphere HA の相互運用性
- vSphere HA クラスタの作成および構成
- vSphere HA クラスタのベスト プラクティス

## vSphere HA の動作

vSphere HA は、仮想マシンとそれが配置されたホストをクラスタにプールすることで、仮想マシンに高可用性を提供します。クラスタ内のホストは監視され、障害発生時には、その故障したホスト上の仮想マシンが別のホスト上で再起動されます。

vSphere HA クラスタを作成すると、1 台のホストがプライマリ ホストとして自動的に選択されます。プライマリ ホストは vCenter Server と通信し、すべての保護された仮想マシンの状態とセカンダリ ホストの状態を監視します。ホスト障害には複数のタイプがあり、プライマリ ホストはその障害を検出して適切な処置を行う必要があります。プライマリ ホストは、障害のあるホストと、ネットワーク パーティションにあるホストやネットワークから隔離されたホストを区別する必要があります。プライマリ ホストは、ネットワークとデータストア ハートビートを使用して障害の種類を確認します。



vSphere HA クラスタ

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_ynopbsu2/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ynopbsu2/uiConfId/49694343/))

## プライマリ ホストとセカンダリ ホスト

ホストを vSphere HA クラスタに追加すると、そのホストにエージェントがアップロードされ、クラスタ内の他のエージェントと通信するように構成されます。クラスタ内の各ホストは、プライマリ ホストまたはセカンダリ ホストとして機能します。

クラスタに対して vSphere HA が有効にされると、アクティブなすべてのホスト（スタンバイ モードやメンテナンス モード以外のホスト、または切断されていないホスト）がクラスタのプライマリ ホストの候補になります。マウントしているデータストア数が最大のホストがマスタ候補として有利です。一般にクラスタごとにプライマリ ホストは 1 台だけで、残りはすべてセカンダリ ホストになります。プライマリ ホストは、障害が発生したり、シャットダウンされたり、スタンバイ モードになったり、クラスタから取り除かれたりした場合、選び直されます。

クラスタのプライマリ ホストには多くの責任があります。

- セカンダリ ホストの状態を監視する。セカンダリ ホストに障害が発生した場合や接続できなくなった場合、プライマリ ホストはどの仮想マシンを再起動する必要があるかを特定します。
- 保護対象の仮想マシンの電源状態を監視する。ある仮想マシンに障害が発生した場合、プライマリ ホストはその仮想マシンを確実に再起動させます。ローカルの配置エンジンを使用して、どのホストで再起動するかもプライマリ ホストが決定します。
- クラスタ ホストと保護対象の仮想マシンのリストの管理。
- vCenter Server の管理インターフェイスとして機能し、クラスタの健全性状態をレポートします。

セカンダリ ホストは、主として仮想マシンをローカルに実行し、ランタイム状態を監視し、状態の更新をプライマリ ホストにレポートすることでクラスタに貢献します。プライマリ ホストも仮想マシンを実行し、監視できます。セカンダリ ホストとプライマリ ホストの両方とも、仮想マシンとアプリケーションの監視機能を実装しています。

プライマリ ホストにより実行される機能の 1 つは、保護された仮想マシンの組織的な再起動です。ユーザー アクションに対応して vCenter Server によって仮想マシンのパワー状態がパワーオフからパワーオンに変わったことが確認されると、仮想マシンはプライマリ ホストによって保護されます。プライマリ ホストは保護された仮想マシンのリストをクラスタのデータストアに保持します。新しく選択されたプライマリ ホストは、この情報を使用してどの仮想マシンを保護するか決定します。

---

**注：** ホストをクラスタから切断する場合、そのホストに登録されている仮想マシンはすべて、vSphere HA の保護対象ではなくなります。

---

## ホスト障害のタイプと検出

vSphere HA クラスタのプライマリ ホストは、セカンダリ ホストの障害検出を行います。検出された障害のタイプによっては、ホストで実行中の仮想マシンのフェイルオーバーが必要になる場合があります。

vSphere HA クラスタでは、3 種類のホスト障害が検出されます。

- 障害 - ホストが機能を停止する。
- 隔離 - ホストがネットワーク隔離される。

- パーティション - ホストがプライマリ ホストとのネットワーク接続を失う。

プライマリ ホストは、クラスタ内のセカンダリ ホストの稼動状態を監視します。この通信は、ネットワーク ハートビートを毎秒、交換することによって行われます。セカンダリ ホストからのハートビートの受信が停止すると、プライマリ ホストはホストの稼動状態を確認してから障害を宣言します。プライマリ ホストは、セカンダリ ホストがデータストアの1つとハートビートを交換しているかどうかを調べて稼動状態を確認します。[データストア ハートビート](#) を参照してください。また、ホストの管理 IP アドレスに送信された ICMP ping に反応するかどうかを確認します。

プライマリ ホストがセカンダリ ホストのエージェントと直接通信できず、セカンダリ ホストが ICMP ping に応答しないことが原因でエージェントからハートビートが送信されない場合、セカンダリ ホストは障害とみなされます。このホストの仮想マシンは、代わりのホスト上で再起動されます。そのようなセカンダリ ホストがデータストアとハートビートを交換している場合、プライマリ ホストは、そのセカンダリ ホストがネットワーク パーティションにあるか、隔離されたネットワークにあると推測し、ホストと仮想マシンの監視を続行します。[ネットワーク パーティション](#) を参照してください。

ホストのネットワークが隔離されるのは、ホストがまだ実行中にも関わらず、管理ネットワーク上で vSphere HA エージェントからのトラフィックを確認できない場合です。ホストがこのトラフィックを確認できなくなった場合は、クラスタの隔離アドレスに ping を試みます。ping にも応答がなかった場合、そのホストは自身をネットワークから隔離されたとみなします。

プライマリ ホストは、隔離されたホストで実行中の仮想マシンを監視します。プライマリ ホストが管理している仮想マシンがパワーオフした場合は、その仮想マシンを再起動します。

---

**注：** ネットワークのインフラストラクチャを冗長にして、少なくとも1つのネットワーク パスを常に使用できるようにしておくと、ネットワークの隔離はほとんど発生しません。

---

## ホスト問題に対する対応の決定

ホストに障害が発生してホストの仮想マシンを再起動する必要がある場合、仮想マシン再起動の優先順位設定で、仮想マシンが起動する順序を制御できます。また、ホスト隔離時の対応設定を使用して、ホストがほかのホストとの管理ネットワークの接続が失われた場合の vSphere HA の対応を構成することもできます。障害発生後に vSphere HA が仮想マシンを再起動するとき、その他の要素も考慮されます。

ホストの障害または隔離時に、次の設定がクラスタ内のすべての仮想マシンに適用されます。特定の仮想マシンに対して例外を設定することも可能です。[個々の仮想マシンのカスタマイズ](#) を参照してください。

### 仮想マシン再起動の優先順位

仮想マシン再起動の優先順位は、ホストの障害後に仮想マシンにリソースを割り当てる相対順位を決定します。このような仮想マシンは、予約されていない容量を使用してホストに割り当てられます。まず優先順位がもっとも高い仮想マシンが配置され、すべての仮想マシンが配置されるか、仮想マシンの予約またはメモリ オーバーヘッドを満たすだけの使用可能なクラスタ容量がなくなるまで、優先順位の順に仮想マシンの配置が続けられます。ホストはその後、割り当てられた仮想マシンをその優先順位の順に再起動します。リソースが不十分であれば、vSphere HA は予約されていない容量がさらに使用可能になる（ホストがオンライン状態に戻るなど）まで待機し、これらの仮想マシン

の配置を再試行します。このような状況が発生する可能性を減らすため、障害に備え、より多くのリソースを予約するように vSphere HA アドミッション コントロールを構成します。アドミッション コントロールにより、仮想マシンによって予約されたクラスタ容量を制御できます。この予約されたクラスタ容量は、障害発生時にその他の仮想マシンの予約およびメモリ オーバーヘッドを満たすためには使用できません。

この設定の値は、次のとおりです。無効、低、中（デフォルト）、および高。無効を選択しても、vSphere HA の仮想マシンとアプリケーションの監視機能で無視されます。これは、この機能により、仮想マシンの障害ではなくオペレーティング システム レベルの障害に対して仮想マシンが保護されるからです。オペレーティング システム レベルの障害が発生すると、vSphere HA によってオペレーティング システムが再起動され、仮想マシンは同じホストで稼動したままになります。この設定は、仮想マシンごとに変更できます。

---

**注：** 仮想マシンをリセットすると、ゲスト OS が強制的に再起動されますが、仮想マシンは電源サイクルされません。

---

仮想マシン再起動の優先順位設定は、ユーザーのニーズによって異なります。最も重要なサービスを提供する仮想マシンに、最も高い再起動の優先順位を割り当てます。

たとえば、多重階層のアプリケーションでは、仮想マシン上にホストされている機能に応じて、割り当てをランク付けすることができます。

- 高：アプリケーションにデータを提供するデータベース サーバ。
- 中：データベースのデータを消費し、その結果を Web ページに提供するアプリケーション サーバ。
- 低：ユーザー要求を受け取り、問い合わせをアプリケーション サーバに渡して、その結果をユーザーに戻す Web サーバ。

ホストに障害が発生すると、vSphere HA は、パワーオンされていて再起動の優先順位設定が無効になっている仮想マシン、またはパワーオフされている、影響を受ける仮想マシンをアクティブなホストに登録しようとします。

## ホストの隔離時の対応

ホスト隔離時の対応で、vSphere HA クラスタ内のホストが管理ネットワークに接続できなくなったものの、実行が継続されている場合の対応を決定します。隔離時の対応を使用して、隔離状態にあるホストで実行されている仮想マシンを vSphere HA でパワーオフし、隔離状態にないホストで再起動することができます。ホスト隔離時の対応では、ホスト監視ステータスを有効にする必要があります。ホスト監視ステータスが無効になっていると、ホスト隔離時の対応もサスペンドされます。ホストは、他のホストで実行中のエージェントと通信できず、隔離アドレスに ping できないときに、自身が隔離されていると判断します。その後、ホストは隔離時の対応を実行します。仮想マシンをパワーオフして再起動、または仮想マシンをシャットダウンして再起動するという対応です。個々の仮想マシンのこのプロパティはカスタマイズできます。

---

**注：** 仮想マシンで再起動の優先順位設定が無効になっていると、ホスト隔離時の対応は行われません。

---

仮想マシンをシャットダウンして再起動する設定を使用するには、仮想マシンのゲスト OS に VMware Tools をインストールする必要があります。仮想マシンをシャットダウンすることには、仮想マシンの状態を保存できるというメリットがあります。ディスクへの最新の変更がフラッシュされず、トランザクションがコミットされないため、仮想マシンのシャットダウンはパワーオフよりも優れています。シャットダウン途中の仮想マシンは、シャットダウンが完了するまでフェイルオーバーに時間がかかります。300 秒以内または詳細オプション

`das.isolationshutdowntimeout` で指定した時間以内にシャットダウンしない仮想マシンは、パワーオフされません。

vSphere HA クラスタを作成したあとで、特定の仮想マシンの再起動優先順位および隔離時の対応についてデフォルトのクラスタ設定をオーバーライドできます。このようなオーバーライドは、特別なタスクで使用される仮想マシンでは非常に便利です。たとえば、DNS や DHCP などのインフラストラクチャ サービスを提供する仮想マシンは、クラスタ内のほかの仮想マシンより前にパワーオンする必要があることがあります。

プライマリ ホストからホストが隔離されるかパーティション化され、プライマリ ホストがハートビート データストアを使用してホストと通信できなくなると、仮想マシンが「スプリット ブレイン」状態になることがあります。この場合、プライマリ ホストはホストが活動中かどうかを判断できないため、ホストが非活動であると宣言します。その後プライマリ ホストは、隔離されているホストまたはパーティション化されているホストで実行されている仮想マシンの再起動を試みます。仮想マシンが隔離/パーティション化されているホスト上で実行されていて、そのホストが隔離されたかパーティション化されたときにそのホストが仮想マシンのデータストアにアクセスできなくなった場合、この再起動の試行は成功します。この後、仮想マシンのインスタンスが 2 つ存在するため、スプリット ブレイン状態が発生します。ただし、1 つのインスタンスのみが仮想マシンの仮想ディスクを読み書きできます。仮想マシンのコンポーネント保護を使用することにより、このスプリット ブレイン状態を防ぐことができます。積極的設定で VMCP を有効にすると、VMCP は、パワーオンされた仮想マシンがデータストアにアクセスできるかどうかを監視し、データストアにアクセスできない仮想マシンをシャットダウンします。

この状況から回復するため、ESXi は、ディスク ロックを失った仮想マシンについて、ホストがいつ隔離状態から離脱してディスク ロックを再取得できなくなったかという問い合わせを生成します。vSphere HA は自動的にこの問い合わせに応答し、ディスク ロックを失った仮想マシンのインスタンスをパワーオフし、ディスク ロックを保持するインスタンスをそのままにします。

## 仮想マシンの再起動に関して考慮される要素

障害発生後、クラスタのプライマリ ホストは障害の影響を受けた仮想マシンをパワーオンできるホストを特定して、障害の影響を受けた仮想マシンの再起動を試みます。このようなホストを選択する場合、プライマリ ホストはいくつもの要素を考慮します。

### ファイルへのアクセス

仮想マシンが起動可能になるには、プライマリがネットワーク経由で通信できるアクティブなクラスタ ホストのいずれかから、仮想マシンのファイルにアクセスする必要があります。

### 仮想マシンとホストとの互換性

アクセス可能なホストが複数存在する場合、仮想マシンは、そのうちの少なくとも 1 台と互換性を持っている必要があります。一連の仮想マシンの互換性には、必要となるすべての仮想マシンとホスト間のアフィニティ ルールの影響が反映されます。たとえばルールにより、2 台のホスト上でのみ仮想マシンの実行を許可している場合、それら 2 台のホストに仮想マシンを配置することが考慮されます。

### リソースの予約

仮想マシンを実行可能なホストのうちの少なくとも 1 台には、仮想マシンのメモリ オーバーヘッドおよび任意のリソース予約に十分な、予約されていない容量が必要です。CPU、メモリ、vNIC、および仮想フラッシュの 4 種類の予約が考慮されます。また、仮想マシンをパワーオンするのに十分なネットワーク ポートも使用可能にする必要があります。

## ホスト制限

リソース予約に加えて、許可される仮想マシン数または使用中の vCPU 数の最大数を超えない場合にのみ、仮想マシンをホストに配置できます。

## 機能の制約

vSphere HA の詳細オプションが、仮想マシンと仮想マシン間の非アフィニティ ルールを強制するように設定されている場合、vSphere HA はこのルールに違反しません。また vSphere HA は、Fault Tolerance 機能を持つ仮想マシンのホストごとに構成された制限のいずれにも違反しません。

上述の考慮事項を満たすホストが存在しない場合、プライマリ ホストは、vSphere HA が仮想マシンを起動するのに必要なリソースがないことを表すイベントを発行し、クラスタの状態が変更されたときに再試行します。たとえば、仮想マシンにアクセスできない場合、プライマリ ホストは、ファイルがアクセス可能になった後に再試行します。

## 仮想マシン再起動の試行回数の制限

vSphere HA プライマリ エージェントが、仮想マシンの登録とパワーオンを含む仮想マシンの再起動を試行して失敗した場合、この再起動は待機時間後に再試行されます。vSphere HA は、これらの再起動を最大試行回数（デフォルトでは 6 回）だけ試行しますが、すべての再起動失敗がこの最大回数にカウントされるわけではありません。

たとえば、再起動の試行が失敗するもっとも一般的な理由は、仮想マシンが別のホストで実行中である、または vSphere HA が再試行を失敗してからすぐに仮想マシンの再起動を試みたためです。このような状況では、プライマリ エージェントは前回の試行で設けられた待機時間の 2 倍の待機時間を設けてから再試行します。最短の待機時間は 1 分間、最長の待機時間は 30 分間です。このため、待機時間が 1 分間に設定されていて、初回の試行が T=0 に行われたとすると、その後の試行は T=1 (1 分後)、T=3 (3 分後)、T=7 (7 分後)、T=15 (15 分後)、T=30 (30 分後) に行われます。このような試行はそれぞれ最大再試行回数にカウントされ、デフォルトで 6 回の試行のみが行われます。

その他の再起動の失敗では、再試行はカウント対象ですが、待機時間の間隔が異なります。このようなシナリオの例は、プライマリ エージェントがホストを選択した後に、仮想マシンの再起動先として選択されたホストが、仮想マシンのいずれかのデータストアにアクセスできなくなった場合です。この場合、再試行はデフォルトの待機時間である 2 分後に行われます。この試行も最大再試行回数にカウントされます。

最後に、カウントされない再試行の例を挙げます。プライマリ エージェントが再起動要求を発行する前に、仮想マシンの再起動先となるホストに障害が発生した場合、2 分後に再試行されますが、この失敗は最大再試行回数にはカウントされません。

## 仮想マシンの再起動の通知

vSphere HA は、クラスタ内の仮想マシンのフェイルオーバー操作が進行中である場合に、クラスタ イベントを生成します。イベントにより、[クラスタ サマリ] タブに構成の問題も表示されます。ここには、再起動される仮想マシン数が表示されます。これらの仮想マシンは 4 つのカテゴリに分類されます。

- 配置されている仮想マシン：vSphere HA は、これらの仮想マシンの再起動を試行しています



- 再試行を待機中の仮想マシン：前回の再起動の試行が失敗したため、vSphere HA は待機中です。待機時間が経過したら再試行します。
- 追加リソースが必要な仮想マシン：これらの仮想マシンを再起動できるだけのリソースが十分ではありません。さらに多くのリソースが使用可能になったとき（ホストがオンライン状態に戻ったとき）に、vSphere HA は再試行します。
- アクセス不能な Virtual SAN 仮想マシン：Virtual SAN 仮想マシンがアクセス不能なため、vSphere HA はこれらの VSAN 仮想マシンを再起動できません。アクセシビリティに変更があったときに再試行します。

実行中の再起動操作が対象とする仮想マシン数に変更が見られた場合は、これらの仮想マシン数が動的に更新されます。vSphere HA がすべての仮想マシンを再起動したか、試行を断念した場合、構成の問題はクリアされます。

vSphere 5.5 以前では、仮想マシンを再起動する試行が失敗すると、仮想マシンごとのイベントがトリガされます。vSphere 6.x ではこのイベントはデフォルトで無効になっていますが、vSphere HA の詳細オプション `das.config.fdm.reportfailoverfailevent` を 1 に設定することで有効にできます。

## 仮想マシンとアプリケーションの監視

仮想マシンの監視では、VMware Tools のハートビートが設定した時間内に受信できなかった場合、その仮想マシンが個別に再起動されます。同様に、実行中のアプリケーションのハートビートが受信できない場合には、アプリケーションの監視によって仮想マシンが再起動されます。これらの機能を有効にし、vSphere HA が無応答を監視する感度を設定できます。

仮想マシンの監視を有効にすると、仮想マシンの監視サービスは（VMware Tools を使用）、ゲスト内で実行される VMware Tools プロセスからの定期的なハートビートおよび I/O アクティビティをチェックして、クラスタ内の各仮想マシンが稼動しているかどうかを判断します。ハートビートや I/O アクティビティが受信されない場合、ほとんどの原因は、ゲスト OS で障害が発生しているか、VMware Tools が割り当てられていないためにタスクが終了できないというものです。このような場合、仮想マシンの監視サービスは、仮想マシンで障害が発生したと判断し、仮想マシンを再起動してサービスを回復させます。

場合によっては、正常に機能している仮想マシンやアプリケーションが、ハートビートの送信を停止することがあります。不必要なリセットを防ぐため、仮想マシンの監視サービスは、仮想マシンの I/O アクティビティも監視しています。障害間隔内にハートビートが受信されなかった場合は、I/O 統計間隔（クラスタレベルの属性）がチェックされます。I/O 統計間隔では、過去 2 分間（120 秒間）に、仮想マシンでディスクまたはネットワーク アクティビティが発生しているかどうかを確認されます。発生していない場合、その仮想マシンはリセットされます。このデフォルト値（120 秒）は、詳細オプション `das.iostatsinterval` を使用して変更できます。

アプリケーションの監視を有効にするには、まず適切な SDK を入手し（または VMware アプリケーションの監視をサポートするアプリケーションを使用中）、これを使用して監視対象となるアプリケーションの、カスタマイズされたハートビートを設定する必要があります。ハートビートを設定したら、アプリケーションの監視は仮想マシンの監視とほぼ同じように機能します。アプリケーションのハートビートが指定した期間受信できないと、仮想マシンは再起動されます。

監視感度のレベルは設定が可能です。監視感度を高度にすると、障害が発生したことが迅速に判断されます。ほとんど起こらないことですが、監視感度を高くすると、対象の仮想マシンまたはアプリケーションが実際には機能しているのに、リソースの制約などによってハートビートが受信されないため、障害であると誤って判断してしまうことがあります。監視感度を低くすると、実際に障害が発生してから仮想マシンがリセットされるまでの間、サービスが中断される時間が長くなります。ニーズに対して効果があるオプションを選択します。

監視感度のデフォルト設定を、表 2-1. 仮想マシンの監視設定 に示します。[カスタム] チェック ボックスを選択すると、監視感度と I/O 統計間隔の両方に、カスタム値を指定することもできます。

表 2-1. 仮想マシンの監視設定

設定	障害間隔 (秒)	リセット間隔
高	30	1 時間
中	60	24 時間
低	120	7 日

障害が検出されると、vSphere HA は仮想マシンをリセットします。リセットすることで、確実にそのサービスが継続して利用可能になります。一時的ではないエラーに対して、仮想マシンが繰り返しリセットされないようにするため、デフォルトでは、仮想マシンは設定可能な特定の期間中に 3 回しかリセットされません。仮想マシンが 3 回リセットされると、vSphere HA は、これ以降に障害が発生しても、指定された時間が経過するまでは仮想マシンをリセットしようとしません。[仮想マシンごとの最大リセット回数] カスタム設定を使用することで、リセット回数を構成できます。

**注：** 仮想マシンをパワーオフしてからパワーオンした場合、または vMotion を使用して別のホストに移行した場合には、リセット統計がクリアされます。これによりゲスト OS が再起動しますが、仮想マシンの電源状態が変更した場合の再起動とは異なります。

仮想マシンでデータストアのアクセシビリティ障害 ([すべてのパスがダウンしています] または [永続的なデバイス損失] のいずれか) が発生すると、仮想マシン監視サービスは、その障害が解決されるまでリセットをサスペンドします。

## 仮想マシン コンポーネント保護

仮想マシンのコンポーネント保護 (VMCP) が有効な場合、vSphere HA はデータストアのアクセス障害を検出して、影響を受ける仮想マシンの自動リカバリを実行できます。

VMCP では、vSphere HA クラスタ内のホストで実行される仮想マシンに影響を与えることがある、データストアのアクセシビリティ障害に対する保護が提供されます。データストアのアクセシビリティ障害が発生すると、影響を受けるホストは、特定データストアのストレージ パスにアクセスできなくなります。このような障害に対して vSphere HA が実行する対応を決定できます。対応はイベント アラームの作成から、別のホスト上での仮想マシンの再起動までの多岐にわたります。

**注：** 仮想マシン コンポーネント保護機能を使用するには、ESXi ホストがバージョン 6.0 以降である必要があります。

## 障害の種類

次に 2 種類のデータストアのアクセシビリティ障害があります。

### PDL

PDL (Permanent Device Loss)。データストアがホストからアクセスできないことをストレージ デバイスが報告するときに発生する、回復不可能なアクセシビリティの喪失です。仮想マシンをパワーオフせずにこの状態を元に戻すことはできません。

## APD

APD (All Paths Down)。一時的または不明なアクセシビリティの喪失、または I/O 処理に見られるその他の識別不可能な遅延です。この種類のアクセスの問題は回復可能です。

## VMCP の構成

仮想マシン コンポーネント保護は vSphere Web Client で構成します。[構成] タブで、[vSphere の可用性]、[編集] の順にクリックします。[障害および対応] では、[PDL (Permanent Device Loss) 状態のデータストア] または [APD 状態のデータストア] を選択できます。選択可能なストレージ保護レベル、および使用可能な仮想マシンの修正操作は、データストアのアクセシビリティ障害の種類に応じて異なります。

### PDL 障害

[PDL (Permanent Device Loss) 状態のデータストア] では、[イベントの発行] または [仮想マシンをパワーオフして再起動] を選択できます。

### APD 障害

APD イベントへの対応はより複雑なため、それに合わせて構成もよりきめ細かくなります。[イベントの発行]、[仮想マシンをパワーオフして再起動: 標準的な再起動ポリシー]、または [仮想マシンをパワーオフして再起動: アグレッシブな再起動ポリシー] を選択できます。

---

**注：** ホストの監視または仮想マシン再起動の優先順位設定のいずれかが無効な場合、VMCP は仮想マシンの再起動を実行できません。ただし、ストレージの健全性を監視し、イベントを発行することができます。

---

## ネットワーク パーティション

vSphere HA クラスタで管理ネットワークの障害が発生すると、そのクラスタのホストの一部は、管理ネットワーク越しに他のホストと通信できなくなる場合があります。クラスタ内に複数のパーティションが発生します。

クラスタがパーティション化されると、仮想マシンの保護やクラスタの管理機能が低下します。パーティション化したクラスタはできるだけ早く修復します。

- 仮想マシンの保護。vCenter Server を使用して仮想マシンをパワーオンできますが、仮想マシンを保護できるのは、その仮想マシンに責任のあるプライマリ ホストと同一パーティションで仮想マシンが実行されている場合のみです。プライマリ ホストは、vCenter Server と通信する必要があります。プライマリ ホストが仮想マシンに対して責任があるのは、その仮想マシンの構成ファイルを含むデータストア上のシステム定義ファイルを排他的にロックしている場合です。
- クラスタ管理。vCenter Server はプライマリ ホストと通信することができますが、セカンダリ ホストは一部のみです。結果的に、vSphere HA に影響する構成変更は、パーティション化が解決されるまで実行されない場合があります。この障害の結果、パーティションの 1 つは古い構成のまま運用され、他のパーティションでは新しい設定が使用されているということが起こり得ます。

## データストア ハートビート

vSphere HA クラスタ内のプライマリ ホストが管理ネットワーク経由でセカンダリ ホストと通信できないとき、プライマリ ホストはデータストア ハートビートを使用して、セカンダリ ホストに障害があるかどうか、セカンダリ ホストがネットワーク パーティションにあるのか、隔離されたネットワークにあるのかを確認します。セカンダリ ホストがデータストア ハートビートを停止している場合は、障害が発生していて、仮想マシンはほかの場所で再起動されているとみなされます。

vCenter Server は、ハートビート用データストアの優先セットを選択します。この選択は、ハートビート データストアにアクセスするホスト数を最大に、データストアが同一 LUN または NFS サーバーにバックアップされる可能性が最小になるように行われます。

詳細オプションの `das.heartbeatdsperhost` を使用して、各ホストの vCenter Server により選択されるハートビート データストアの数を変更できます。デフォルトは 2 で、有効最大値は 5 です。

vSphere HA は各データストアのルートにディレクトリを作成します。このディレクトリは、データストア ハートビートおよび保護された仮想マシンのセット保持の両方に使用されます。ディレクトリ名は `.vSphere-HA` です。動作に影響することがあるので、このディレクトリに格納されたファイルを削除したり変更したりしないでください。複数のクラスタが 1 つのデータストアを使用している場合に備え、各クラスタ用にこのディレクトリのサブディレクトリが作成されます。これらのディレクトリとファイルの所有者はルート (root) であり、これらのディレクトリやファイルを読み書きできるのはルートのみです。vSphere HA によって使用されるディスク スペースは、使用される VMFS のバージョンやハートビート用にデータストアを使用するホスト数など、いくつかの要因で決まります。vmfs3 では、最大使用量は約 2GB で、通常の使用量は 3MB 程度です。vmfs5 では、最大使用量と通常の使用量は約 3MB です。vSphere HA がデータストアを使用することによるオーバーヘッドは無視できる程度で、他のデータストア処理のパフォーマンスには影響しません。

vSphere HA では、1 つのデータストアに構成ファイルを持つことのできる仮想マシンの数が制限されます。制限の更新については、『構成の上限』を参照してください。データストアにこの数を超える仮想マシンを配置してパワーオンした場合、制限数の仮想マシンまでしか vSphere HA によって保護されません。

---

**注：** Virtual SAN データストアは、データストア ハートビートには使用できません。したがって、他の共有ストレージがクラスタのすべてのホストにアクセスできない場合、使用中のハートビート データストアは存在しない可能性があります。ただし、Virtual SAN ネットワークとは独立した代替のネットワーク パスによってアクセスできるストレージがある場合、それを用いてハートビート データストアを設定できます。

---

## vSphere HA セキュリティ

vSphere HA は、いくつかのセキュリティ機能により拡張されます。

### 開いているファイアウォールのポートを選択

vSphere HA は、TCP および UDP ポート 8182 をエージェント間の通信に使用します。ファイアウォールのポートの開閉は自動で、必要なときだけ開くようになっています。

### ファイル システム権限を使用して保護された構成ファイル

vSphere HA は、ローカル データストアがない場合、構成情報をローカル ストレージまたは RAM ディスクに格納します。これらのファイルは、ファイル システム権限を使用して保護されており、root ユーザーだけがア

クセス可能です。ローカル ストレージがないホストは、Auto Deploy で管理される場合にのみサポートされます。

## 詳細なログ

vSphere HA がログ ファイルを置く場所は、ホストのバージョンによって異なります。

- ESXi 5.x ホストでは、vSphere HA が syslog に書き込むのはデフォルトの場合のみで、ログは、syslog で構成された場所に置かれます。vSphere HA 用のログ ファイル名には、vSphere HA のサービスの 1 つであるフォールト ドメイン マネージャを表す `fdm` が前に付加されています。
- レガシー ESXi 4.x ホストでは、vSphere HA は、syslog のほかにローカル ディスクの `/var/log/vmware/fdm` にも書き込みます（そのように構成されている場合）。
- レガシー ESX 4.x ホストでは、vSphere HA は `/var/log/vmware/fdm` に書き込みます。

## vSphere HA へのセキュアなログイン

vSphere HA は、vCenter Server により作成されたユーザー アカウントである `vpxuser` を使用して、vSphere HA エージェントにログオンします。このアカウントは、vCenter Server がホストを管理するために使用するのと同じアカウントです。vCenter Server はこのアカウント用にランダムなパスワードを作成し、定期的に変更します。その期間は、vCenter Server の `VirtualCenter.VimPasswordExpirationInDays` 設定で設定します。ホストのルート フォルダの管理権限を持つユーザーは、このエージェントにログインできます。

## セキュアな通信

vCenter Server と vSphere HA エージェント間の通信は、すべて SSL 経由で行われます。エージェント間の通信も SSL を使用しますが、(マスター ホスト) 選択メッセージの通信だけは UDP 経由で行われます。選択メッセージは SSL で検証されるため、プライマリ ホストになることを不正なエージェントが妨害できるのは、そのエージェントが実行されているホストだけです。このケースでは、クラスタの構成に問題があることが通知され、ユーザーに注意を促します。

## Host SSL 証明書の検証が必要

vSphere HA では、各ホストに検証済みの SSL 証明書があることが必要です。各ホストは、最初に起動したときに自己署名の証明書を生成します。次に、この証明書は再生成されるか、認証局が発行した証明書に置き換えられます。証明書が置き換えられた場合、ホスト上で vSphere HA を再構成する必要があります。証明書が更新されて ESXi または ESX ホスト エージェントが再起動した後にホストが vCenter Server から切断された場合は、vCenter Server に再接続されたときに vSphere HA は自動的に再構成されます。vCenter Server ホストの SSL 証明書の検証が無効なため切断されなかった場合は、新しい証明書を検証してホスト上の vSphere HA を再構成します。

## vSphere HA のアドミッション コントロール

vCenter Server はアドミッション コントロールを使用することで、フェイルオーバー保護を提供できるだけの十分なリソースをクラスタ内に確保し、仮想マシンのリソース予約が必ず順守されるようにします。

3 つのタイプのアドミッション コントロールを使用できます。

## ホスト

ホスト上で実行されるすべての仮想マシンの予約を満たすのに十分なリソースを、そのホストに確保します。

## リソース プール

リソース プールに関連付けられたすべての仮想マシンの予約、シェア、制限を満たすのに十分なリソースを、そのリソース プールに確保します。

## vSphere HA

ホストで障害発生時に仮想マシンをリカバリするための、十分なリソースがクラスタ内で必ず予約されるようにします。

アドミッション コントロールでは、リソース使用率が制約され、その制約に違反するすべてのアクションが禁止されます。禁止されるアクションとしては、次のようなものがあります。

- 仮想マシンのパワーオン。
- ホスト、クラスタ、リソース プールへの仮想マシンの移行。
- 仮想マシンの CPU またはメモリ予約の増加。

3 つのタイプのアドミッション コントロールの中で、無効にできるのは vSphere HA アドミッション コントロールのみです。ただし、このアドミッション コントロールを有効にしておかないと、障害発生後に予想どおりの数の仮想マシンが再起動する保証が得られません。アドミッション コントロールを永続的に無効にしないでください。ただし、次のような場合は一時的に無効にする必要があります。

- フェイルオーバーをサポートできるだけの十分なリソースがなく、フェイルオーバー制約に違反する必要がある場合（ホストをスタンバイ モードにして DPM（Distributed Power Management）の使用をテストするときなど）。
- 自動プロセスで、一時的にフェイルオーバー制約に違反する可能性のあるアクションを実行する必要がある場合（vSphere Update Manager の指示による ESXi ホストのアップグレードまたはパッチ適用の一部など）。
- テストまたはメンテナンス操作を実行する必要がある場合。

アドミッション コントロールは容量を別に確保しますが、障害が発生すると仮想マシンの再起動に利用できるすべての容量が vSphere HA で使用されます。たとえば、vSphere HA は、ユーザーが開始するパワーオンに対してアドミッション コントロールで許可されている以上の仮想マシンをホストに配置します。

---

**注：** vSphere HA アドミッション コントロールが無効なとき、vSphere HA は、DPM が有効で仮想マシンすべてを 1 つのホストに統合できる場合でも、クラスタ内に少なくとも 2 つのパワーオン ホストが確実にあるようにします。これによって確実にフェイルオーバーが可能になります。

---

## クラスタで許容するホスト障害アドミッション コントロール ポリシー

vSphere HA を構成して、指定した数のホスト障害を許容できます。クラスタで許容するホスト障害アドミッション コントロール ポリシーでは、vSphere HA により、指定された数のホストで障害が発生しても、それらのホストからすべての仮想マシンにフェイルオーバーするのに十分なリソースがクラスタ内に残ります。

クラスタで許容するホスト障害ポリシーでは、vSphere HA によって次のアドミッション コントロールが実行されます。

#### 1 スロット サイズを計算します。

スロットは、メモリおよび CPU リソースの論理的な表現方法です。デフォルトで、クラスタ内でパワーオンされている仮想マシンの要件を満たすよう、サイズが調整されます。

#### 2 クラスタ内の各ホストが保持できるスロットの数を決定します。

#### 3 クラスタの現在のフェイルオーバー キャパシティを決定します。

これは障害が発生し、パワーオン状態のすべての仮想マシンの要件を満たす十分なスロットが残っている可能性があるホストの数です。

#### 4 現在のフェイルオーバー キャパシティが、(ユーザーが定義した) 構成済みフェイルオーバー キャパシティよりも少ないかどうか判断します。

少ない場合、アドミッション コントロールにより操作が禁止されます。

---

**注：** vSphere Web Client の vSphere HA 設定のアドミッション コントロールのセクションで、CPU とメモリの両方について具体的なスロット サイズを設定できます。

---

## スロット サイズの計算



vSphere HA のスロット サイズとアドミッション コントロール

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_q744qxvn/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_q744qxvn/uiConfId/49694343/))

スロット サイズは、CPU とメモリの 2 つのコンポーネントで構成されます。

- vSphere HA では、パワーオン状態の各仮想マシンの CPU 予約を取得し、最も大きな値を選択することによって、CPU コンポーネントを計算します。仮想マシンの CPU 予約を指定していない場合、デフォルト値である 32MHz が割り当てられます。das.vmcputminmhz という詳細オプションで、この値を変更できます。
- vSphere HA では、パワーオン状態の各仮想マシンのメモリ予約 (にメモリ オーバーヘッドを加えた値) を取得し、最も大きな値を選択することによって、メモリ コンポーネントを計算します。メモリ予約には、デフォルト値はありません。

クラスタの中に、ほかよりもかなり多い予約が割り当てられている仮想マシンが含まれている場合は、スロット サイズの計算が正確になりません。このような問題を回避するために、das.slotcpuinmhz または das.slotmeminmb の詳細オプションを使用して、スロット サイズの CPU コンポーネントまたはメモリ コンポーネントに対する上限をそれぞれ指定できます。[vSphere HA の詳細オプション](#)を参照してください。

また、複数のスロットを必要とする仮想マシンの数を表示することで、クラスタ内のリソースの断片化のリスクを判断することもできます。これは、vSphere Web Client の vSphere HA 設定のアドミッション コントロールのセクションで計算できます。詳細オプションを使用して固定のスロット サイズや最大のスロット サイズを指定している場合、仮想マシンで複数のスロットが必要になる場合があります。

## スロットを使用した現在のフェイルオーバー キャパシティの計算

スロット サイズが計算されると、vSphere HA は、仮想マシンで使用できる各ホストの CPU とメモリのリソースを決定します。これらの量は、ホストの物理リソースの合計ではなく、ホストのルート リソース プールに含まれています。vSphere HA で使用されるホストのリソース データは、vSphere Web Client のホストの [サマリ] タブにあります。クラスタ内のホストがすべて同一の場合、このデータは、クラスタレベルの数字をホスト数で割れば得られます。仮想化のために使用中のリソースは除外されます。接続されていてメンテナンス モードでなく、vSphere HA エラーがないホストのみが考慮されます。

次に、各ホストがサポートできるスロットの最大数が決定されます。そのためには、ホスト CPU のリソース量をスロット サイズの CPU コンポーネントで割り、結果を切り捨てます。ホストのメモリ リソース量に対して、同じ計算が行われます。これらの 2 つの値が比較され、小さい方が、ホストがサポートできるスロット数になります。

現在のフェイルオーバー キャパシティは、何台のホスト（最も大きいものから開始）で障害が発生する可能性があるか、およびパワーオン状態のすべての仮想マシンの要件を満たす十分なスロットが残っているかを判定することによって計算されます。

### 詳細ランタイム情報

クラスタで許容するホスト障害アドミSSION コントロール ポリシーを選択すると、[詳細ランタイム情報] ペーンが、vSphere Web Client のクラスタの [監視] タブの vSphere HA セクションに表示されます。このペーンには、クラスタに関する次の情報が表示されます。

- スロット サイズ。
- クラスタ内のスロット総数。クラスタ内の正常ホストでサポートされるスロット総数。
- 使用済みスロット。パワーオン状態の仮想マシンに割り当てられているスロット数。詳細オプションを使用して、スロット サイズに上限を定義している場合は、パワーオン状態の仮想マシンの数を超えることがあります。これは、一部の仮想マシンが複数のスロットを占有しているからです。
- 使用可能なスロット。クラスタ内の他の仮想マシンをパワーオンする際に使用できるスロットの数。vSphere HA は、フェイルオーバーに必要なスロット数を予約します。それ以外のスロットは、新しい仮想マシンのパワーオンに使用できます。
- フェイルオーバー スロット。使用済みのスロットや利用可能なスロットをカウントしない総スロット数。
- クラスタ内でパワーオン状態にある仮想マシンの総数。
- クラスタ内のホスト総数。
- クラスタ内の正常ホスト総数。接続されていて、メンテナンス モードでなく、vSphere HA エラーの生じていないホスト数。

### 例：クラスタで許容するホスト障害ポリシーを使用したアドミSSION コントロール

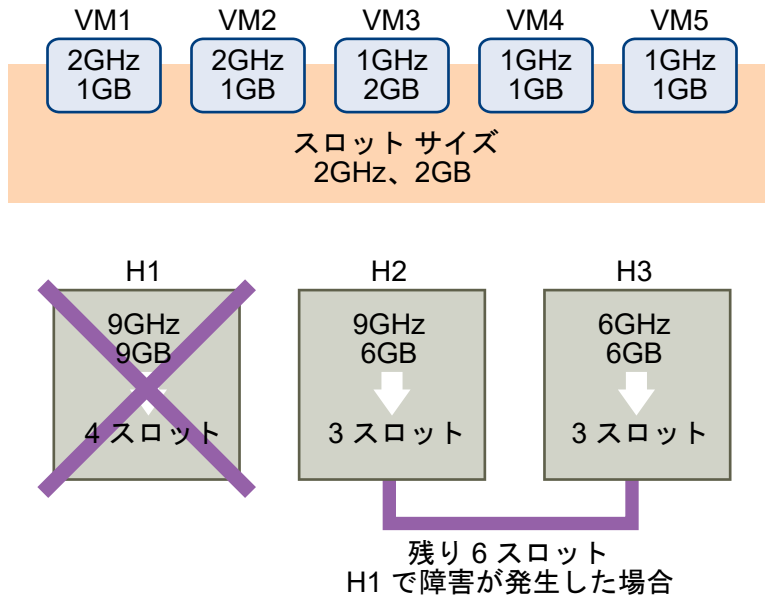
この例では、スロット サイズがどのように計算され、このアドミSSION コントロール ポリシーでどのように使用されるかを示します。クラスタについて次のように仮定します。

- クラスタは 3 台のホストで構成されており、それぞれ異なる量の、使用可能な CPU リソースとメモリ リソースがあります。最初のホスト（H1）は、使用可能な 9GHz の CPU リソースと 9GB のメモリがありますが、ホスト 2（H2）には、9GHz の CPU リソースと 6GB のメモリ、ホスト 3（H3）には 6GHz の CPU リソースと 6GB のメモリがあります。



- クラスタ内には、パワーオン状態の仮想マシンが 5 台あり、それぞれに異なる CPU 要件とメモリ要件があります。VM1 は 2GHz の CPU リソースと 1GB のメモリが必要ですが、VM2 は 2GHz の CPU リソースと 1GB のメモリ、VM3 は 1GHz の CPU リソースと 2GB のメモリ、VM4 は 1GHz の CPU リソースと 1GB のメモリ、VM5 は 1GHz の CPU リソースと 1GB のメモリが必要です。
- クラスタで許容するホスト障害は 1 に設定されます。

図 2-1. クラスタで許容するホスト障害ポリシーによるアドミSSION コントロールの例



- 1 仮想マシンの CPU 要件とメモリ要件の両方で比較を行なって最大の値を選択することにより、スロット サイズが計算されます。

最大の CPU 要件は 2GHz (VM1 と VM2 で共通) で、最大のメモリ要件は 2GB (VM3 の) です。これらの値に基づいて、スロット サイズは 2GHz CPU および 2GB メモリになります。

- 2 各ホストでサポートできるスロットの最大数を決定します。

H1 は 4 つのスロットをサポートできます。H2 は 3 スロット (9GHz/2GHz および 6GB/2GB の小さい方)、H3 も 3 スロットをサポートできます。

- 3 現在のフェイルオーバー キャパシティを計算します。

最も大きいホストは H1 で、H1 で障害が発生しても、クラスタでは 6 つのスロットを使用できます。これは、パワーオン状態の 5 台の仮想マシンすべてに対して十分なスロットです。H1 と H2 の両方で障害が発生すると、3 つのスロットしか使用できなくなり、これでは不十分です。したがって、現在のフェイルオーバー キャパシティは 1 になります。

クラスタには、使用できるスロットが 1 つあります (H2 と H3 の 6 つのスロットから、使用済みの 5 つのスロットを減算する)。

## 予約されたクラスタ リソースの割合アドミSSION コントロール ポリシー

ホスト障害からのリカバリ用にクラスタ CPU およびメモリ リソースの一定割合を予約することで、アドミSSION コントロールが実行できるよう、vSphere HA を構成できます。

予約されたクラスタ リソースの割合アドミッション コントロール ポリシーでは、vSphere HA によって、CPU とメモリのリソース総量のうち、指定した割合がフェイルオーバー用に予約されます。

予約されたクラスタ リソース ポリシーでは、vSphere HA によって次のアドミッション コントロールが実行されます。

- 1 クラスタ内のパワーオン状態のすべての仮想マシンに対する、リソース要件の合計を計算します。
- 2 仮想マシンで利用できるホスト リソースの合計を計算します。
- 3 クラスタの現在の CPU フェイルオーバー キャパシティおよび現在のメモリ フェイルオーバー キャパシティを計算します。
- 4 現在の CPU フェイルオーバー キャパシティ、または現在のメモリ フェイルオーバー キャパシティのいずれかが、(ユーザーが定義した) 対応する構成済みフェイルオーバー キャパシティより小さいかどうかを判断します。

いずれかが小さい場合は、アドミッション コントロールにより操作が禁止されます。

vSphere HA では、仮想マシンの実際の予約が使用されます。仮想マシンに予約がない、つまり予約が 0 の場合は、デフォルトの OMB のメモリおよび 32MHz の CPU が適用されます。

---

**注：** 予約されたクラスタ リソースの割合アドミッション コントロール ポリシーでは、クラスタ内に少なくとも 2 つの vSphere HA 対応ホストがあることを確認します (メンテナンス モードに入っているホストを除く)。vSphere HA 対応のホストが 1 つしかない場合、利用可能なリソースの割合が十分であっても実行できません。この確認を追加するのは、クラスタ内にホストが 1 つしかない場合、vSphere HA はフェイルオーバーを実行できないからです。

---

## 現在のフェイルオーバー キャパシティの計算

パワーオン状態の仮想マシンに対するリソース要件の合計は、CPU とメモリの 2 つのコンポーネントで構成されます。vSphere HA は、これらの値を計算します。

- パワーオン状態の仮想マシンの CPU 予約量を合計することによる、CPU コンポーネントの値。仮想マシンの CPU 予約が指定されていない場合は、デフォルト値の 32MHz が割り当てられます (この値は、`das.vmcputminmhz` 詳細オプションを使用して変更できます)。
- パワーオン状態の各仮想マシンのメモリ予約 (およびメモリ オーバーヘッド) を合計することによる、メモリ コンポーネントの値。

仮想マシンで利用できるホスト リソースの合計は、ホストの CPU リソースとメモリ リソースを合計して計算されます。これらの量は、ホストの物理リソースの合計ではなく、ホストのルート リソース プールに含まれています。仮想化のために使用中のリソースは除外されます。メンテナンス モードではない接続状態のホストで、vSphere HA のエラーがないホストのみが対象となります。

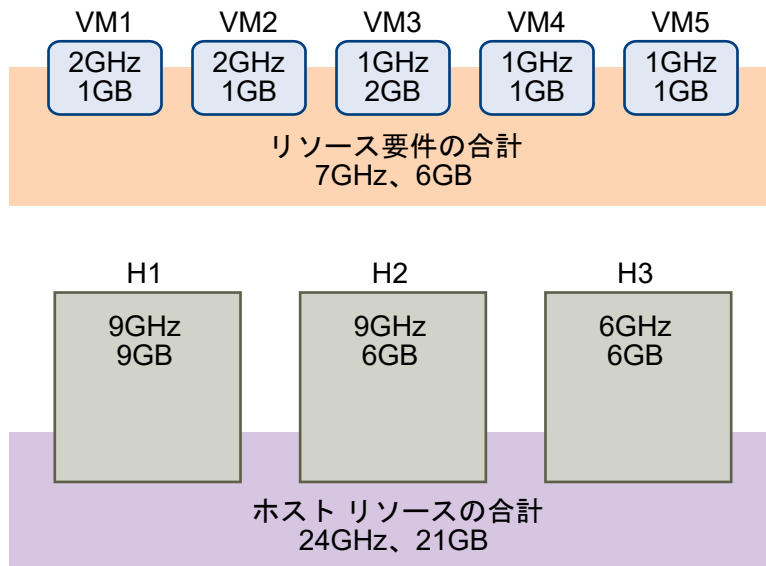
現在の CPU フェイルオーバー キャパシティは、ホスト CPU リソースの合計から、CPU リソース要件の合計を減算し、その結果の値を、ホスト CPU リソースの合計で除算した値になります。現在のメモリ フェイルオーバー キャパシティも同様に計算されます。

## 例：予約されたクラスタ リソースの割合ポリシーを使用したアドミッション コントロール

この例では、現在のフェイルオーバー キャパシティがどのように計算され、このアドミッション コントロール ポリシーでどのように使用されるかを示します。クラスタについて次のように仮定します。

- クラスタは 3 台のホストで構成されており、それぞれ異なる量の、使用可能な CPU リソースとメモリ リソースがあります。最初のホスト（H1）は、使用可能な 9GHz の CPU リソースと 9GB のメモリがありますが、ホスト 2（H2）には、9GHz の CPU リソースと 6GB のメモリ、ホスト 3（H3）には 6GHz の CPU リソースと 6GB のメモリがあります。
- クラスタ内には、パワーオン状態の仮想マシンが 5 台あり、それぞれに異なる CPU 要件とメモリ要件があります。VM1 は 2GHz の CPU リソースと 1GB のメモリが必要ですが、VM2 は 2GHz の CPU リソースと 1GB のメモリ、VM3 は 1GHz の CPU リソースと 2GB のメモリ、VM4 は 1GHz の CPU リソースと 1GB のメモリ、VM5 は 1GHz の CPU リソースと 1GB のメモリが必要です。
- CPU とメモリの構成済みフェイルオーバー キャパシティはいずれも 25% に設定されています。

図 2-2. 予約されたクラスタ リソースの割合ポリシーを使用したアドミッション コントロールの例



パワーオン状態の仮想マシンに対するリソース要件の合計は、CPU リソースが 7GHz、メモリが 6GB です。仮想マシンで利用できるホスト リソースの合計は、CPU リソースが 24GHz、メモリが 21GB です。これに基づいて、現在の CPU フェイルオーバー キャパシティは 70%  $((24\text{GHz} - 7\text{GHz}) / 24\text{GHz})$  となります。同様に、現在のメモリ フェイルオーバー キャパシティは 71%  $((21\text{GB} - 6\text{GB}) / 21\text{GB})$  になります。

クラスタの構成済みフェイルオーバー キャパシティは 25% に設定されているため、クラスタの CPU リソースの合計の 45%、およびクラスタのメモリ リソースの 46% は、追加の仮想マシンをパワーオンするために使用できます。

## フェイルオーバー ホストの指定アドミッション コントロール ポリシー

特定のホストをフェイルオーバー ホストとして指定するように vSphere HA を構成できます。

フェイルオーバー ホストの指定アドミッション コントロール ポリシーでは、ホストで障害が発生したときに、vSphere HA が、指定されたフェイルオーバー ホストのいずれかで障害ホストの仮想マシンを再起動しようとしません。フェイルオーバー ホスト自身で障害が発生している、または十分なリソースがない、などの理由で再起動できない場合、vSphere HA はこれらの仮想マシンを、クラスタ内の別のホストで再起動しようとしません。

フェイルオーバー ホストで予備のキャパシティを確実に使用できるようにするため、仮想マシンをパワーオンすること、または vMotion を使用して仮想マシンをフェイルオーバー ホストに移行することはできません。また、DRS はロード バランシング用としてフェイルオーバー ホストを使用しません。

---

**注：** フェイルオーバー ホストの指定アドミッション コントロール ポリシーを使用して複数のフェイルオーバー ホストを指定する場合、DRS はフェイルオーバー ホストで実行されている仮想マシンについて仮想マシン間のアフィニティ ルールを強制的に実行しようとしません。

---

現在のフェイルオーバー ホストが、クラスタの [サマリ] タブにある vSphere HA セクションに表示されます。各ホストの隣のステータス アイコンは、緑、黄色、赤のいずれかになります。

- 緑：ホストが接続されている状態で、メンテナンス モードではなく、vSphere HA のエラーはありません。このホストには、パワーオン状態の仮想マシンは存在しません。
- 黄色：ホストが接続されている状態で、メンテナンス モードではなく、vSphere HA のエラーはありません。ただし、このホストには、パワーオン状態の仮想マシンが存在しています。
- 赤：ホストが切断されている状態で、メンテナンス モードであるか、vSphere HA のエラーがあります。

## アドミッション コントロール ポリシーの選択

vSphere HA のアドミッション コントロール ポリシーは、可用性のニーズ、およびクラスタの特性に基づいて選択する必要があります。アドミッション コントロール ポリシーを選択する場合は、いくつかの事項を考慮する必要があります。

### リソースの断片化の回避

リソースの断片化が発生するのは、フェイルオーバーの対象となる仮想マシンに対して、全体のリソースは十分であるものの、個々のリソースが複数のホストに分散しており、リソースを使用できない場合です。これは、1 台の仮想マシンは同時に 1 台の ESXi ホスト上でしか稼動できないためです。クラスタで許容するホスト障害ポリシーのデフォルト構成では、仮想マシンの最大予約量として 1 つのスロットを定義することにより、リソースの断片化を回避します。クラスタ リソースの割合ポリシーは、リソースの断片化の問題について対処しません。フェイルオーバー ホストの指定ポリシーでは、フェイルオーバーに対してホストが予約されるため、リソースは断片化されません。

### フェイルオーバー リソースの予約に関する柔軟性

それぞれのアドミッション コントロール ポリシーでは、フェイルオーバーの保護に対してクラスタ リソースを予約する場合のコントロールの細かさが異なります。クラスタで許容するホスト障害ポリシーでは、フェイルオーバー レベルをホストの数として設定できます。クラスタ リソースの割合ポリシーでは、フェイルオーバーに対し、クラスタの CPU またはメモリ リソースを最大 100% まで指定できます。フェイルオーバー ホストの指定ポリシーでは、フェイルオーバー ホストの組を指定できます。

## クラスタの異種性

仮想マシンのリソース予約、およびホストのリソース キャパシティの合計については、クラスタは異種であってもかまいません。異種クラスタでは、クラスタで許容するホスト障害ポリシーにおいて、許容する程度がかなり低くなる場合があります。このポリシーでは、スロット サイズを定義する場合に仮想マシンの最大の予約量しか考慮せず、現在のフェイルオーバー キャパシティを計算する場合に、最大のホストで障害が発生することを仮定しているためです。ほかの 2 つのアドミッション コントロール ポリシーは、クラスタの異種性によって影響されません。

---

**注：** vSphere HA は、アドミッション コントロールの計算を実行する場合に、Fault Tolerance のセカンダリ仮想マシンのリソース使用量を含めます。クラスタで許容するホスト障害ポリシーでは、セカンダリ仮想マシンにスロット が割り当てられ、クラスタ リソースの割合ポリシーでは、クラスタで使用可能なキャパシティを計算するとき、セカンダリ仮想マシンのリソース使用率が計上されます。

---

## vSphere HA の相互運用性

vSphere HA は、DRS や Virtual SAN などの他の多くの機能と相互運用できます。

vSphere HA を構成する前に、これらの他の機能または製品との相互運用性の制限について理解しておく必要があります。

## vSphere HA と Virtual SAN の併用

Virtual SAN を vSphere HA クラスタの共有ストレージとして使用できます。有効にすると、Virtual SAN はホストの利用可能なローカル ストレージ ディスクの中で指定したものを、すべてのホストで共有される単一のデータストアに統合します。

vSphere HA を Virtual SAN と併用するには、これらの両機能の相互運用性についていくつかの注意事項や制限事項を理解しておく必要があります。

Virtual SAN の詳細については、『VMware Virtual SAN』を参照してください。

## ESXi ホストの要件

Virtual SAN は、次の条件を満たす場合にのみ vSphere HA クラスタと併用できます。

- クラスタの ESXi ホストはすべてバージョン 5.5 以降である必要があります。
- クラスタには、3 つ以上の ESXi ホストが必要です。

## ネットワークの相違点

Virtual SAN には独自のネットワークがあります。Virtual SAN と vSphere HA が同じクラスタに対して有効にされていると、HA のエージェント間のトラフィックは管理ネットワークではなくこのストレージ ネットワークを通過します。Virtual SAN が無効のときだけ、vSphere HA は管理ネットワークを使用します。vSphere HA がホストで構成されているとき、vCenter Server は適切なネットワークを選択します。

---

**注：** vSphere HA が無効のときだけ、Virtual SAN を有効にできます。

---

Virtual SAN のネットワーク構成を変更すると、vSphere HA エージェントは新しいネットワーク設定を自動的に取得しません。したがって、Virtual SAN のネットワークに変更を加えるには、vSphere Web Client で次の手順を実行する必要があります。

- 1 vSphere HA クラスタの [ホストの監視] を無効にします。
- 2 Virtual SAN ネットワークに変更を加えます。
- 3 クラスタのすべてのホストを右クリックし、[vSphere HA 用に再構成] を選択します。
- 4 vSphere HA クラスタの [ホストの監視] を有効に戻します。

表 2-2. vSphere HA ネットワークの相違点 に、Virtual SAN が使用されているときと使用されていないときの vSphere HA ネットワークの相違点を示します。

表 2-2. vSphere HA ネットワークの相違点

	Virtual SAN 有効時	Virtual SAN 無効時
vSphere HA が使用するネットワーク	Virtual SAN ストレージ ネットワーク	管理ネットワーク
ハートビート データストア	2 つ以上のホストにマウントされる、Virtual SAN データストア以外のデータストア	2 つ以上のホストにマウントされるデータストア
ホストは「隔離」と宣言	隔離アドレスは ping 不可、Virtual SAN ストレージ ネットワークはアクセス不可	隔離アドレスは ping 不可、管理ネットワークはアクセス不可

## 容量の予約設定

vSphere HA クラスタにアドミSSION コントロール ポリシーで容量を予約する場合、この設定は、障害時にデータのアクセシビリティを確保する Virtual SAN の対応する設定と関係させる必要があります。特に、Virtual SAN のルール セットの [許容する障害の数] の設定は、vSphere HA アドミSSION コントロールの設定で予約されている容量よりも低くすることはできません。

たとえば、Virtual SAN のルール セットが 2 つの障害しか許容していない場合、vSphere HA アドミSSION コントロール ポリシーでは 1 つまたは 2 つのホスト障害に相当する容量を予約する必要があります。ホストが 8 台あるクラスタで [予約されたクラスタ リソースの割合] ポリシーを使用している場合、クラスタ リソースの 25% を超えて予約をしないでください。同じクラスタで、[ホスト障害のクラスタ許容] ポリシーを使用してホストの台数が 2 を超えないように設定します。vSphere HA によって予約される容量が少なすぎると、フェイルオーバーが期待されたとおりに動作しない可能性があります。一方、過度に大きな容量が予約されると、仮想マシンのパワーオンとクラスタ間の vMotion 移行に大きな制約が生じることがあります。

## vSphere HA と DRS の併用

vSphere HA を DRS (Distributed Resource Scheduler) と組み合わせて使用すると、自動フェイルオーバーとロード バランシングの両方が実現されます。この組み合わせにより、vSphere HA が仮想マシンを別のホストに移行したあとのクラスタはバランスが向上します。

vSphere HA がフェイルオーバーを実行し、異なるホスト上で仮想マシンを再起動する場合、最優先事項は、すべての仮想マシンの当面の可用性にあります。仮想マシンが再起動されたあと、それらの仮想マシンがパワーオンされたホストは負荷が大きくなる場合があるのに対し、ほかのホストは負荷が比較的軽くなります。vSphere HA は、仮想マシンの CPU とメモリの予約とオーバーヘッド メモリを使用して、仮想マシンに対応できる十分なキャパシティがホストにあるかどうかを判断します。

DRS および vSphere HA を使用するクラスタでアドミッション コントロールがオンになっている場合、メンテナンス モードに入るホストから仮想マシンを退避できないことがあります。これは、障害時の仮想マシンの再起動用にリソースが予約されているために発生します。vMotion を使用して、手動でホストから仮想マシンを移行する必要があります。

いくつかのシナリオでは、リソースの制約が原因で、vSphere HA が仮想マシンをフェイルオーバーできない場合があります。これが生じる理由はいくつかあります。

- HA アドミッション コントロールが無効になっていて、DPM (Distributed Power Management) が有効になっている場合。これにより、DPM が少数のホストに仮想マシンを統合し、空のホストをスタンバイ モードにするため、パワーオン状態のキャパシティが不足してフェイルオーバーを行えなくなります。
- 仮想マシンとホスト間のアフィニティ (必須) ルールによって、特定の仮想マシンを配置できるホストが制限される場合がある。
- 十分な集約リソースはあっても、複数のホスト間で断片化される可能性があるため、仮想マシンでフェイルオーバーに使用できない場合。

このような場合、vSphere HA は DRS を使用してクラスタの調整を試み (ホストのスタンバイ モードを終了したり、仮想マシンを移行してクラスタ リソースを最適化したりするなど)、HA がフェイルオーバーを実行できるようにします。

DPM が手動モードの場合、ホストのパワーオンの推奨を確認する必要がある場合があります。同様に、DRS が手動モードの場合は、移行の推奨を確認する必要がある場合があります。

仮想マシンとホスト間の必須のアフィニティ ルールを使用している場合は、これらのルールに違反できないことを理解しておく必要があります。vSphere HA は、フェイルオーバーの実行がこのようなルールの違反につながる場合は、フェイルオーバーを行いません。

DRS の詳細については、『vSphere リソース管理』ドキュメントを参照してください。

## vSphere HA および DRS のアフィニティ ルール

クラスタに DRS アフィニティ ルールを作成すると、仮想マシンのフェイルオーバー中に vSphere HA がそのルールをどのように適用するかを指定できます。

vSphere HA のフェイルオーバーの動作に指定できる 2 種類のルールを以下に挙げます。

- フェイルオーバー アクション中、指定された仮想マシンをフェイルオーバーに参加させない、仮想マシン非アフィニティ ルール。
- フェイルオーバー アクション中、指定された仮想マシンを特定のホストまたは定義されたホスト グループのメンバーに配置する、仮想マシンとホスト間のアフィニティ ルール。

DRS アフィニティ ルールを編集するとき、vSphere HA に必要なフェイルオーバー動作を実行するチェックボックスを選択します。

- [HA はフェイルオーバー中に仮想マシン非アフィニティ ルールを順守する必要があります] : このルールが指定された仮想マシンと一緒に配置されている場合、フェイルオーバーは停止されます。



- [HA はフェイルオーバー中に仮想マシンとホスト間のアフィニティ ルールを順守する必要があります] :  
vSphere HA は、このルールが指定された仮想マシンを、できる限り指定されたホストに配置するように試みます。

---

**注：** ルールを設定した直後（デフォルトで 5 分以内）にホストの障害が発生した場合、vSphere HA は、仮想マシンとホスト間のアフィニティ ルールのマッピングを無視して、DRS が無効なクラスタ内の仮想マシンを再起動できます。

---

## vSphere HA の相互運用性に関するその他の問題

vSphere HA を使用するには、次に示す、相互運用性に関するその他の問題について理解しておく必要があります。

### 仮想マシン コンポーネント保護

仮想マシン コンポーネント保護 (VMCP) には、次に示す相互運用性の問題と制限があります。

- VMCP は vSphere Fault Tolerance をサポートしていません。Fault Tolerance を使用しているクラスタで VMCP を有効にすると、影響を受ける FT 仮想マシンは、VMCP を無効にするオーバーライドを自動的に受け取ります。
- VMCP は、Virtual SAN データストアに配置されているファイルのアクセシビリティ問題を検出したり、それに応答したりしません。仮想マシンの構成ファイルと VMDK ファイルが Virtual SAN データストアにのみ配置されている場合は、VMCP によって保護されません。
- VMCP は、仮想ボリューム データストアに配置されているファイルのアクセシビリティ問題を検出したり、それに応答したりしません。仮想マシンの構成ファイルと VMDK ファイルが仮想ボリューム データストアにのみ配置されている場合、それらのファイルは VMCP によって保護されません。
- VMCP は、アクセス不可の RAW デバイス マッピング (RDM) に対する保護は行いません。

### IPv6

vSphere HA は IPv6 ネットワーク構成で 사용할 수ことができ、次の考慮事項が守られている場合に完全にサポートされます。

- クラスタには、ESXi 6.0 以降のホストのみが含まれています。
- クラスタのすべてのホストの管理ネットワークは、同じ IP バージョン (IPv6 または IPv4 のどちらか) で構成されている必要があります。vSphere HA クラスタに両方のタイプのネットワーク構成を含めることはできません。
- vSphere HA によって使用されるネットワーク隔離アドレスは、管理ネットワークでクラスタによって使用される IP バージョンと一致する必要があります。
- IPv6 は、Virtual SAN も使用されている vSphere HA クラスタで 사용할 수することはできません。

上記の制限事項に加えて、アドレス タイプがリンクローカル、ORCHID、および ゾーン インデックスのリンクローカルである IPv6 アドレスは、vSphere HA 隔離アドレスまたは管理ネットワークで 사용할 수ようにはサポートされていません。また、管理ネットワークでループバック アドレス タイプを使用することはできません。

---

**注：** 既存の IPv4 デプロイを IPv6 にアップグレードするには、まず vSphere HA を無効にする必要があります。

---



## vSphere HA クラスタの作成および構成

vSphere HA は、ESXi（または、レガシー ESX）ホストのクラスタのコンテキストで機能します。フェイルオーバーの保護を確立するには、事前にクラスタを作成し、そのクラスタにホストを配置して、vSphere HA の設定を構成しておく必要があります。

vSphere HA のクラスタを作成する場合には、機能がどのように作用するかを決定する多数の設定を構成する必要があります。これを実行する前に、クラスタのノードを確認します。これらのノードは、仮想マシンをサポートするリソースを提供する ESXi ホストで、vSphere HA は、これらのホストをフェイルオーバーの保護のために使用します。次に、これらのノードが互いにどのように接続されるか、および仮想マシンのデータが格納されている共有ストレージに対してどのように接続されるかを決定します。このネットワーク アーキテクチャが整備されると、クラスタにホストを追加し、vSphere HA の構成を完了できます。

クラスタに対してホスト ノードを追加する前に、vSphere HA を有効にして構成できます。ただし、クラスタにホストが追加されるまで、クラスタは十分に機能せず、クラスタの設定の中には使用できないものもあります。たとえば、フェイルオーバー ホストとして指定できるホストが存在しない場合は、フェイルオーバー ホストの指定アドミSSION コントロール ポリシーは使用できません。

---

**注：** 仮想マシンの起動およびシャットダウン（自動起動）の機能は、vSphere HA クラスタ内にある（またはこのクラスタ内に移行された）ホスト上のすべての仮想マシンで無効になっています。vSphere HA とともに使用されるとき、自動起動はサポートされません。

---

## vSphere HA のチェックリスト

vSphere HA のチェックリストでは、vSphere HA クラスタを作成および使用する前に理解しておく必要のある要件について説明しています。

vSphere HA クラスタをセットアップする前に、次の内容を確認してください。詳細については、該当するクロスリファレンスを参照してください。

- すべてのホストに vSphere HA のライセンスがある。
- クラスタには、ホストが少なくとも 2 つ含まれている必要があります。
- すべてのホストは、固定 IP アドレスで構成する必要があります。DHCP を使用している場合は、再起動しても各ホストのアドレスが変わらないことを確認する必要があります。
- すべてのホストに、少なくとも 1 つの共通の管理ネットワークが必要です。ベスト プラクティスでは、共通の管理ネットワークを 2 つ以上構成します。VMkernel ネットワークを、[管理トラフィック] チェックボックスが有効での状態で使用する必要があります。各ネットワークは相互にアクセス可能になっており、管理ネットワークで vCenter Server とホストが相互にアクセス可能になっている必要があります。[ネットワークのベスト プラクティス](#) を参照してください。

- クラスタ内の任意のホストで任意の仮想マシンを実行できるようにするために、すべてのホストから同じ仮想マシンのネットワークおよびデータストアにアクセスできるようになっている必要があります。同様に、仮想マシンはローカル以外の共有ストレージに配置する必要があります。共有できない場合は、ホストの障害時に仮想マシンはフェイルオーバーされません。

---

**注：** vSphere HA は、データストア ハートビートを使用して、パーティション化されたホスト、隔離されたホスト、および障害のあるホストを区別します。したがって、使用環境で一部のデータストアの信頼性が高い場合は、それらを優先するように vSphere HA を構成します。

---

- 仮想マシンの監視が機能するために、VMware Tools がインストールされている。[仮想マシンとアプリケーションの監視](#) を参照してください。
- vSphere HA は IPv4 および IPv6 の両方をサポートしています。IPv6 を使用する場合は考慮事項については、[vSphere HA の相互運用性に関するその他の問題](#) を参照してください。
- 仮想マシン コンポーネント保護が正常に機能するには、ホストで全パスダウン (APD) タイムアウト機能を有効にする必要があります。
- 仮想マシン コンポーネント保護を使用するには、クラスタに ESXi 6.0 以降のホストが含まれている必要があります。
- VMCP を有効にするために使用できるのは、ESXi 6.0 以降のホストが含まれている vSphere HA クラスタのみです。以前のリリースのホストを含むクラスタでは VMCP を有効にできません。また、それらのホストは VMCP が有効なクラスタに追加できません。
- クラスタで仮想ボリューム データストアを使用する場合、vSphere HA が有効にされると、vCenter Server により各データストアで構成仮想ボリュームが作成されます。vSphere HA は、これらのコンテナに、仮想マシンの保護に使用するファイルを保存します。これらのコンテナを削除すると、vSphere HA が正常に機能しなくなります。コンテナは、仮想ボリューム データストアごとに 1 つだけ作成されます。

## vSphere HA クラスタの作成

vSphere HA 用にクラスタを有効にするには、最初に空のクラスタを作成する必要があります。クラスタのリソースおよびネットワーク アーキテクチャの計画後に、vSphere Web Client を使用してクラスタにホストを追加し、そのクラスタの vSphere HA 設定を指定します。

Fault Tolerance には vSphere HA 対応のクラスタが必須です。

### 前提条件

- すべての仮想マシンとその構成ファイルが共有ストレージに格納されていることを確認します。
- クラスタ内の別のホストを使用して仮想マシンをパワーオンできるようにするため、ホストが共有ストレージにアクセスするように構成されていることを確認します。
- ホストが仮想マシン ネットワークにアクセスできるよう構成されていることを確認します。
- vSphere HA 用に冗長な管理ネットワーク接続を使用していることを確認します。ネットワークの冗長性の設定に関する詳細は、[ネットワークのベスト プラクティス](#) を参照してください。
- vSphere HA データストア ハートビートに冗長性を持たせるため、少なくとも 2 つのデータストアを使用してホストが構成されていることを確認します。

- クラスタの管理者権限を持つアカウントを使用して、vSphere Web Client を vCenter Server に接続します。

#### 手順

- 1 vSphere Web Client で、クラスタを配置するデータセンターを参照し、[クラスタの作成] をクリックします。
- 2 [新規クラスタ] ウィザードを最後まで実行します。  
vSphere HA (または DRS) を有効にしないでください。
- 3 [OK] をクリックしてウィザードを閉じ、空のクラスタを作成します。
- 4 クラスタのリソースおよびネットワーク アーキテクチャの計画に基づき、vSphere Web Client を使用してクラスタにホストを追加します。
- 5 クラスタを参照し、vSphere HA を有効にします。
  - a [管理] タブをクリックして、[設定] をクリックします。
  - b [vSphere HA] を選択し、[編集] をクリックします。
  - c [vSphere HA をオンにする] チェック ボックスを選択します。
- 6 [ホスト監視] を選択します。  
ホスト監視を有効にすることにより、クラスタのホストはネットワークのハートビートを相互に送信でき、vSphere HA は障害を検出したときにアクションを実行できます。vSphere Fault Tolerance リカバリ プロセスが正常に機能するには、ホスト監視が必要です。
- 7 [仮想マシンの監視] の設定を選択します。  
[仮想マシンの監視のみ] を選択し、仮想マシンのハートビートを設定した時間内に受信できなくなった場合に、その仮想マシンを個別に再起動します。[仮想マシンとアプリケーションの監視] を選択してアプリケーションの監視を有効にすることもできます。
- 8 [OK] をクリックします。

#### 結果

これで、ホストが組み込まれた vSphere HA クラスタは作成しました。

#### 次のステップ

クラスタについて、vSphere HA 設定を適切に構成します。

- 障害状態と仮想マシンの対応
- アドミSSION コントロール
- ハートビート用のデータストア
- 詳細オプション

[vSphere HA クラスタ設定の構成](#) を参照してください。

## vSphere HA クラスタ設定の構成

vSphere HA のクラスタを作成したり既存のクラスタを構成したりする場合は、機能の動作方法を決める設定を構成する必要があります。

vSphere Web Client では、次の vSphere HA の設定を構成できます。

### 障害状態と仮想マシンの対応

ここでは、仮想マシンの再起動優先順位、ホストの隔離時の応答、仮想マシンの監視感度、および仮想マシン コンポーネント保護の設定を行います。

### アドミSSION コントロール

vSphere HA クラスタに対してアドミSSION コントロールを有効または無効にしたり、アドミSSION コントロールをどのように実行するかポリシーを選択したりします。

### ハートビート用のデータストア

vSphere HA がデータストア ハートビートに使用するデータストアの環境設定を指定します。

### 詳細オプション

詳細オプションを設定して、vSphere HA の動作をカスタマイズします。

**注：** 各ホストでの vSphere HA 構成タスクのステータスは、vSphere Web Client の [タスク] コンソールで確認できます。

## 仮想マシンの対応の構成

[障害状態と仮想マシンの対応] ページでは、ホストの障害と隔離に対して vSphere HA がどのように応答するかを決める設定を選択できます。これらの設定には、仮想マシンの再起動優先順位、ホストの隔離時の対応、仮想マシンのコンポーネント保護の設定、および仮想マシン監視感度などがあります。

[仮想マシンの応答] ページは、vSphere HA を有効にした場合にのみ編集可能になります。

### 手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] をクリックします。
- 4 [障害状態と仮想マシンの対応] を展開して構成オプションを表示します。

オプション	説明
仮想マシン再起動の優先順位	再起動の優先順位は、ホストの障害時に仮想マシンを再起動する順序を特定します。優先順位の高い仮想マシンが先に起動されます。この優先順位はホスト単位でのみ適用されます。複数のホストで障害が発生した場合、優先順位が 1 位のホストからすべての仮想マシンを移行し、次に優先順位が 2 位のホストからすべての仮想マシンを移行するといったように、順次移行を行います。
ホスト隔離への対応	ホストの隔離時の対応では、vSphere HA クラスタ内のホストがコンソール ネットワーク接続を切断されても実行され続ける場合に、どのような処理を行うかを特定します。

オプション	説明
永続的なデバイス損失 (PDL) 状態のデータストアへの対応	この設定により、PDL 障害の場合の VMCP の応答が決まります。[イベントの発行] または [仮想マシンをパワーオフして再起動] を選択できます。
全バス ダウン (APD) 状態のデータストアへの対応	この設定により、APD 障害の場合の VMCP の応答が決まります。[イベントの発行] するように設定するか、保守的または積極的なアプローチで [仮想マシンをパワーオフして再起動] するかをいずれかを選択できます。
APD に対応する仮想マシン フェイルオーバーの遅延時間	この設定は、VMCP がアクションを実行するまでの待機時間（分単位）です。
APD タイムアウト後に APD から回復する場合の対応	この状況で VMCP によって仮想マシンをリセットするかどうかを選択できます。
仮想マシン監視の感度	[低] と [高] の間でスライダを移動して設定します。[カスタム] を選択してカスタム設定を行うこともできます。

## 5 [OK] をクリックします。

### 結果

[仮想マシンの応答] の設定が有効になります。

## アドミSSION コントロールの構成

クラスタを作成したあとでアドミSSION コントロールを使用して、仮想マシンが可用性の制約に違反した場合、その仮想マシンを開始できるかどうかを指定できます。指定した台数のホストに配置された実行中の仮想マシンすべてをフェイルオーバーできるように、クラスタはリソースを予約します。

アドミSSION コントロール ページは、vSphere HA を有効にした場合のみ表示されます。

### 手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] をクリックします。
- 4 [アドミSSION コントロール] を展開して構成オプションを表示します。
- 5 アドミSSION コントロールのポリシーを選択してクラスタに適用します。

オプション	説明
静的なホストの数によるフェイルオーバー キャパシティを定義	復旧可能なホスト障害またはフェイルオーバーを保証するホスト障害の最大数を選択します。また、スロット サイズ ポリシーも選択する必要があります。
クラスタ リソースの割合を予約することによるフェイルオーバー キャパシティの定義	フェイルオーバーをサポートする予備キャパシティとして予約する、クラスタの CPU およびメモリ リソースの割合を指定します。
専用のフェイルオーバー ホストの使用	フェイルオーバー処理に使用するホストを選択します。デフォルトのフェイルオーバー ホストに十分なリソースがない場合でも、フェイルオーバー処理はクラスタ内のほかのホストで行えます。
フェイルオーバー キャパシティを予約しない	このオプションを使用すると、可用性の制約に違反する仮想マシンのパワーオンが可能になります。

6 [OK] をクリックします。

#### 結果

アドミッション コントロールが有効になり、選択したポリシーが有効になります。

### ハートビート用のデータストアの構成

vSphere HA は、データストア ハートビートを使用して、障害が発生したホストとネットワーク パーティションに存在するホストを区別します。データストア ハートビートを使用すると、管理ネットワーク パーティションが発生したときに vSphere HA でホストを監視し、発生したエラーに継続的に応答できます。

データストア ハートビートに使用するデータストアを指定できます。

#### 手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] をクリックします。
- 4 [ハートビート用のデータストア] を展開して、データストア ハートビートの構成オプションを表示します。
- 5 データストアの選択方法と環境設定の処理方法について vSphere HA に指示するには、次のオプションから選択します。

表 2-3.

#### データストア ハートビートのオプション

[ホストからアクセス可能なデータストアを自動的に選択します]

[指定したリストからのデータストアのみを使用する]

[指定したリストからのデータストアを使用し、必要に応じて自動的に補足する]

- 6 [使用可能なハートビート データストア] ペインで、ハートビートに使用するデータストアを選択します。

一覧表示されるのは、vSphere HA クラスタ内の複数のホストで共有されるデータストアです。データストアを選択すると、そのデータストアにアクセスできる vSphere HA クラスタ内のホストがすべてペインの下部に表示されます。

- 7 [OK] をクリックします。

### 詳細オプションの設定

vSphere HA の動作をカスタマイズするには、vSphere HA の詳細オプションを設定します。

#### 前提条件

クラスタの管理者権限があることを確認します。

**注：** これらのオプションは vSphere HA の機能に影響を与えるため、変更には注意が必要です。

## 手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [vSphere HA] を選択し、[編集] をクリックします。
- 4 [詳細オプション] を展開します。
- 5 [追加] をクリックし、詳細オプションの名前をテキスト ボックスに入力します。  
値の列のテキスト ボックスでオプションの値を設定できます。
- 6 追加する新しい各オプションについてステップ 5 を繰り返し、[OK] をクリックします。

## 結果

クラスタはユーザーが追加または変更したオプションを使用します。

## 次のステップ

vSphere HA の詳細オプションを設定すると、次のいずれかの操作を実行するまでそのままになります。

- vSphere Web Client を使用することにより、その値をデフォルト値にリセットする。
- クラスタ内のすべてのホストの fdm.cfg ファイルで、オプションを手動で編集または削除する。

## vSphere HA の詳細オプション

vSphere HA クラスタの動作を指定する詳細オプションを設定できます。

表 2-4. vSphere HA の詳細オプション

オプション	説明
<code>das.isolationaddress[...]</code>	ホストがネットワークから隔離されているかどうかを判断するため、ping を送信するアドレスを設定します。クラスタ内でほかのどのホストからもハートビートが受信されない場合にのみ、このアドレスに ping が送信されます。このアドレスが指定されていない場合は、管理ネットワークのデフォルト ゲートウェイが使用されます。このデフォルト ゲートウェイには、利用可能で信頼性の高いアドレスを指定します。これにより、ネットワークから隔離されているかどうかをホスト自身で判断することができます。クラスタには複数の隔離アドレス (10 個まで) を指定できます : <code>das.isolationaddressX</code> (X は 0 ~ 9)。通常は、管理ネットワークごとに 1 つ指定する必要があります。複数のアドレスを指定すると、隔離の検出に時間がかかります。
<code>das.usedefaultisolationaddress</code>	デフォルトでは、vSphere HA はコンソール ネットワークのデフォルト ゲートウェイを隔離アドレスとして使用します。デフォルトが使用されるかどうかをこのオプションで指定します (true または false)。
<code>das.isolationshutdowntimeout</code>	システムがパワーオフする前に、仮想マシンがシャットダウンするまで待機する時間を設定します。これはホストの隔離時の対応が、仮想マシンのシャットダウンの場合のみ適用されます。デフォルト値は 300 秒です。

表 2-4. vSphere HA の詳細オプション（続き）

オプション	説明
<code>das.slotmeminmb</code>	メモリ スロット サイズの上限を定義します。このオプションが使用されると、スロット サイズは、この値、またはクラスタ内でパワーオン状態になっているあらゆる仮想マシンの最大メモリ予約にメモリ オーバーヘッドを加えた値よりも小さくなります。
<code>das.slotcpuinmhz</code>	CPU スロット サイズの上限を定義します。このオプションが使用されると、スロット サイズは、この値、またはクラスタ内でパワーオン状態になっているあらゆる仮想マシンの最大 CPU 予約よりも小さくなります。
<code>das.vmmemoryminmb</code>	メモリ予約が指定されていない、またはゼロの場合に、仮想マシンに割り当てるデフォルトのメモリ リソース値を定義します。これは、クラスタで許容するホスト障害アドミッション コントロール ポリシーで使用されます。値が指定されていない場合、デフォルトは 0 MB になります。
<code>das.vmcputuminmhz</code>	CPU 予約が指定されていない、またはゼロの場合に、仮想マシンに割り当てるデフォルトの CPU リソース値を定義します。これは、クラスタで許容するホスト障害アドミッション コントロール ポリシーで使用されます。値が指定されていない場合、デフォルトは 32MHz になります。
<code>das.iostatsinterval</code>	仮想マシンの監視感度に対するデフォルトの I/O 統計間隔を変更します。デフォルトは 120（秒）です。0 以上の任意の値を設定できます。0 に設定した場合は、チェックが行われません。  <b>注：</b> 50 未満の値は推奨されません。より小さい値を指定すると、vSphere HA が予期せずに仮想マシンをリセットする可能性があるためです。
<code>das.ignoreinsufficienthbdatastore</code>	ホストに vSphere HA 用の十分なハートビート データストアがない場合、作成された構成の問題を無効にします。デフォルト値は <code>false</code> です。
<code>das.heartbeatdsperhost</code>	データストアが必要とするハートビート数を変更します。有効な値は 2 ～5 の範囲で、デフォルトは 2 です。
<code>das.config.fdm.isolationPolicyDelaySec</code>	ホストが隔離されていると判断された場合に、隔離ポリシーを実行する前にシステムが待機する秒数。最小値は 30 です。30 未満の値に設定しても、遅延時間は 30 秒になります。
<code>das.respectvmvmtiaffinityrules</code>	vSphere HA によって、仮想マシン間の非アフィニティ ルールが強制されるかどうかを決定します。デフォルト値は「 <code>false</code> 」であり、ルールは強制されません。「 <code>true</code> 」に設定して、(vSphere DRS が有効になっていない場合でも) ルールを強制させることもできます。この場合、vSphere HA は仮想マシンをフェイルオーバーするとルールに反する場合はフェイルオーバーを実行しませんが、フェイルオーバーを実行するためのリソースが不足していることをレポートするイベントを発行します。  非アフィニティ ルールの詳細については、『vSphere リソース管理ガイド』を参照してください。
<code>das.maxresets</code>	VMCP が行うリセット試行回数の最大値です。APD (All Paths Down) 状態の影響を受ける仮想マシンでリセット操作が失敗すると、VMCP は処理を終了するまでにこの回数のリセットを試行します。



表 2-4. vSphere HA の詳細オプション（続き）

オプション	説明
<code>das.maxterminates</code>	VMCP が行う仮想マシン終了の最大再試行回数です。
<code>das.terminatere retryintervalsec</code>	VMCP が仮想マシンを終了できない場合に、システムが終了を再試行するまでに待機する時間（秒）です。
<code>das.config.fdm.reportfailoverfailevent</code>	1 に設定すると、vSphere HA が仮想マシンを再起動しようとして失敗したときに、仮想マシンごとの詳細なイベントを生成できます。デフォルト値は 0 です。vSphere 6.0 より前のバージョンでは、このイベントはデフォルトで生成されます。
<code>vpXD.das.completemetadadataupdateintervalsec</code>	仮想マシンとホスト間のアフィニティ ルールが設定されてから、DRS が無効なクラスターで vSphere HA がルールを無視して仮想マシンを再起動できる時間（秒）。デフォルト値は 300 秒です。
<code>das.config.fdm.memReservationMB</code>	<p>デフォルトで vSphere HA エージェントは、メモリの上限 250 MB が構成された状態で実行されます。予約可能なキャパシティが不足している場合、ホストはこの予約を割り当てられないことがあります。この詳細オプションを使用してメモリの上限を減らすことで、この問題を回避できます。100 より大きい整数（最小値）のみを指定できます。反対に、(6,000 から 8,000 台の仮想マシンを含む) 大規模なクラスターでプライマリ エージェントの選択中に発生する問題を回避するには、この制限を 325 MB に増やします。</p> <p><b>注：</b> この上限が変更されると、クラスター内のすべてのホストに対して HA の再構成タスクを実行する必要があります。また、新しいホストがクラスターに追加されたり、既存のホストが再起動されるときに、そのホストに対してこのタスクを実行して、このメモリ設定を更新する必要があります。</p>
<code>das.respectvmhostsoftaffinityrules</code>	同じ仮想マシン ホスト グループに属しているホスト上の各仮想マシンを vSphere HA が再起動するかどうかを決定します。そのような使用可能なホストがない場合、またはこのオプションの値が "false" に設定されている場合、vSphere HA はクラスターで使用可能なすべてのホスト上の仮想マシンを再起動します。vSphere 6.0 では、デフォルト値は「false」です。この値は、クラスターの詳細 HA オプションでは視覚的に定義されていない可能性があります。このオプションを有効にする場合は、クラスターの詳細 HA オプションで手動で「true」に設定する必要があります。

**注：** 次の詳細オプションのいずれかの値を変更する場合、変更を有効にするには vSphere HA を無効にしてから再度有効にする必要があります。

- `das.isolationaddress[...]`
- `das.usedefaultisolationaddress`
- `das.isolationshutdowntimeout`

## 個々の仮想マシンのカスタマイズ

vSphere HA クラスター内の各仮想マシンには、仮想マシン再起動の優先順位、ホスト隔離時の対応、仮想マシンのコンポーネント保護、および仮想マシンの監視に対するクラスターのデフォルト設定が割り当てられます。これらのデ

フォルトを変更すると、仮想マシンごとに特定の動作を指定できます。仮想マシンがそのクラスタから離れると、これらの設定は失われます。

#### 手順

- 1 vSphere Web Client で、vSphere HA クラスタに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [設定] で [仮想マシンのオーバーライド] を選択し、[追加] をクリックします。
- 4 [+] ボタンを使用して、オーバーライドを適用する仮想マシンを選択します。
- 5 [OK] をクリックします。
- 6 (オプション) [自動化レベル]、[仮想マシン再起動の優先順位]、[ホスト隔離時の対応]、VMCP 設定、[仮想マシンの監視]、または[仮想マシンの監視感度]などの設定を変更できます。

---

**注：** まず [関連するクラスタ設定] を展開してから [vSphere HA] を展開することで、これらの設定についてクラスタのデフォルトを表示できます。

---

- 7 [OK] をクリックします。

#### 結果

これで、変更した各設定に関するこの仮想マシンの動作が、クラスタのデフォルトとは異なったものになります。

## vSphere HA クラスタのベスト プラクティス

vSphere HA クラスタのパフォーマンスを最適化するには、特定のベスト プラクティスに従う必要があります。このセクションでは特に、vSphere HA クラスタの主要なベスト プラクティスをいくつか取り上げます。

詳細については、発行ドキュメント『vSphere High Availability Deployment Best Practices』を参照することもできます。

### ネットワークのベスト プラクティス

vSphere HA 用にホストの NIC とネットワーク トポロジを構成するには、次のベスト プラクティスを確認してください。ベスト プラクティスには、ESXi ホストや、配線、スイッチ、ルータ、ファイアウォールに対する推奨事項があります。

#### ネットワークの構成とメンテナンス

次のネットワーク メンテナンスに関する提案は、vSphere HA のハートビートが失われたためにホスト障害やネットワークの隔離を偶発的に検出するのを避けるのに役立ちます。

- クラスタリングされた ESXi ホストが存在するネットワークに変更を加えるときは、ホスト監視機能をサスペンドしてください。ネットワーク ハードウェアまたはネットワーク設定を変更すると、vSphere HA がホスト障害の検出に使用するハートビートが中断することがあり、仮想マシンの不要なフェイルオーバーが行われることがあります。

- ポート グループの追加、vSwitch の削除など、ESXi ホスト自体のネットワーク構成を変更するときは、ホスト監視をサスペンドしてください。ネットワーク構成を変更したあとは、クラスタ内のすべてのホストで vSphere HA を再構成する必要があります。これにより、ネットワーク情報が再検査されます。次に、ホスト監視を再び有効にします。

**注：** ネットワークは vSphere HA の重要なコンポーネントであるため、ネットワークのメンテナンスを実行する必要がある場合は、vSphere HA の管理者に知らせます。

## vSphere HA の通信に使用されるネットワーク

vSphere HA の動作に影響を与えるネットワーク操作を調べるには、ハートビートなどの vSphere HA の通信にどの管理ネットワークが使用されているかを知る必要があります。

- クラスタ内の レガシー ESX ホストでは、サービス コンソール ネットワークとして指定されたすべてのネットワークを、vSphere HA の通信が通過します。VMkernel ネットワークは、これらのホストで vSphere HA の通信に使用されません。ESX コンソール ネットワークのサブセットへの vSphere HA トラフィックを含めるには、`allowedNetworks` 詳細オプションを使用します。
- クラスタの ESXi ホストでは、vSphere HA の通信はデフォルトで VMkernel ネットワークを通過します。ESXi ホストで、vSphere HA のホストと通信するために、vCenter Server が使用するネットワーク以外のネットワークを使用する場合は、[管理トラフィック] チェックボックスを明示的に有効にする必要があります。

vSphere HA エージェントのトラフィックを指定したネットワーク上にとどめるために、vSphere HA が使用する vmkNIC とほかの目的で使用される vmkNIC でサブネットを共有しないようにホストを設定します。vSphere HA エージェントは、vSphere HA 管理トラフィック用に構成された vmkNIC が 1 つ以上ある場合、指定されたサブネットに関連付けられている物理 NIC を使用してパケットを送信します。したがって、ネットワーク フローを確実に分離するには、vSphere HA が使用する vmkNIC と他の機能で使用する vmkNIC を異なるサブネットに配置する必要があります。

## ネットワーク隔離アドレス

ネットワーク隔離アドレスとは、ホストがネットワークから隔離されているかどうかを判断するために ping が行われる IP アドレスです。このアドレスに ping が行われるのは、ホストがクラスタ内のほかのすべてのホストからハートビートを受信しなくなった場合のみです。ホストがこのネットワーク隔離アドレスに ping 可能な場合、そのホストはネットワークから隔離されておらず、クラスタ内のほかのホストで障害が発生しているか、ネットワーク パーティション分割されています。一方、ホストが隔離アドレスに ping 不可能な場合、そのホストはネットワークから隔離されている可能性が高く、フェイルオーバー動作が行われません。

デフォルトでは、そのホストのデフォルト ゲートウェイがネットワーク隔離アドレスになります。管理ネットワークがいくつ定義されていても、デフォルトのゲートウェイとして指定されるのは 1 つだけです。追加ネットワーク用に隔離アドレスを追加するには、`das.isolationaddress[...]` 詳細オプションを使用する必要があります。

[vSphere HA の詳細オプション](#)を参照してください。

## ネットワーク パスの冗長性

クラスタ ノード間のネットワーク パスの冗長性は、vSphere HA の信頼性にとって重要です。単一の管理ネットワークの場合は単一点障害となるため、そのネットワークで障害が発生しただけで、フェイルオーバーが生じることがあります。管理ネットワークが1つしかない場合、ネットワーク障害時にハートビート データストア接続が保持されないと、ホストおよびクラスタ間で発生するすべての障害が、不要な（誤った）フェイルオーバーの原因となることがあります。そうした障害としては、NIC の故障、ネットワーク ケーブルの不良、ネットワーク ケーブルの外れ、スイッチのリセットなどがあります。このようなホスト間の障害の原因をよく検討し、ネットワークに冗長性を持たせるなどして、障害を最小限に抑制してください。

ネットワークの冗長性は、まず、NIC チーミングによって NIC レベルで実装できます。別々の物理スイッチに接続されている 2 つの NIC によるチームを使用すると、管理ネットワークの信頼性が向上します。2 つの NIC を介して（および別々のスイッチを介して）接続されているサーバは、ハートビートを送受信する 2 つの独立したパスを持っているため、クラスタの信頼性が向上します。管理ネットワークに NIC チームを構成するには、有効またはスタンバイの構成の vSwitch 構成で vNIC を構成します。推奨される vNIC のパラメータ設定は、次のとおりです。

- デフォルトのロード バランシング = 発信元のポート ID に基づいたルート
- フェイルバック = なし

vSphere HA クラスタのホストに NIC を追加したあと、そのホストで vSphere HA を再構成する必要があります。

ほとんどの実装で、NIC チーミングは十分なハードビートの冗長性を確保しますが、別の方法として、別の仮想スイッチに接続する 2 番目の管理ネットワーク接続を作成することもできます。冗長な管理ネットワークでは、複数のネットワークを介してハートビートを送信できるため、信頼性の高い障害検出が可能になり、隔離状態またはパーティション状態の発生を防ぐことができます。元の管理ネットワーク接続は、ネットワークおよび管理の目的で使用します。2 番目の管理ネットワーク接続を作成すると、vSphere HA は両方の管理ネットワーク接続でハートビートを送信します。いずれかのパスに障害が発生しても、vSphere HA は、もう一方のパスでハートビートを送受信します。

---

**注：** クラスタ内のサーバ間で、できるだけ少ない数のハードウェア セグメントを構成します。これは、単一点障害を制限することが目的です。また、ルートのホップ数が多すぎる場合も、ハートビート用のネットワーク パケット遅延の原因となり、障害点が増加します。

---

## IPv6 ネットワーク構成の使用

vSphere HA クラスタによって使用される所定のネットワーク インターフェイスに、1 つの IPv6 アドレスのみを割り当てます。複数の IP アドレスを割り当てても、クラスタのプライマリ ホストから送信されるハートビート メッセージ数が増えるだけで、それに伴う利点はありません。

## 相互運用性のベスト プラクティス

vSphere HA と他の機能との間で適切な相互運用性を可能にするには、次のベスト プラクティスを確認してください。

## 混在クラスタにおける vSphere HA および Storage vMotion の相互運用性

ESXi 5.x ホストと ESX/ESXi 4.1 以前のホストが存在するクラスタ、および Storage vMotion が広範に使用されるか ストレージ DRS が有効になっているクラスタの場合、vSphere HA をデプロイしないでください。vSphere HA がホストの障害に応答し、障害が発生する前に仮想マシンが実行されていたときと ESXi バージョンが異なるホストで仮想マシンを再起動する可能性があります。障害発生時に、仮想マシンが ESXi 5.x ホスト上での Storage vMotion アクションに関連していて、vSphere HA が ESXi 5.0 より前のバージョンのホストで仮想マシンを再起動した場合、問題が生じることがあります。仮想マシンはパワーオンする可能性があります、続くスナップショット処理で試みられる操作が vdisk 状態を破損し、仮想マシンが利用できないままになる恐れがあります。

## vSphere HA を使用した Auto Deploy の使用

vSphere HA と Auto Deploy を合わせて使用し、仮想マシンの可用性を向上させることができます。Auto Deploy はホストがパワーオンする際にホストをプロビジョニングします。また、ブート時にそのようなホスト上の vSphere HA エージェントをインストールするように構成することも可能です。詳細については、『vSphere Installation and Setup』に含まれている Auto Deploy ドキュメントを参照してください。

## Virtual SAN を使用したクラスタ内のホストのアップグレード

vSphere HA クラスタ内の ESXi ホストをバージョン 5.5 以上にアップグレードし、さらに Virtual SAN も使用したい場合は、次のプロセスに従います。

- 1 すべてのホストをアップグレードします。
- 2 vSphere HA を無効にします。
- 3 Virtual SAN を有効にします。
- 4 vSphere HA を再度有効にします。

## アドミSSION コントロールのベスト プラクティス

vSphere HA 用のアドミSSION コントロールを構成して使用するには、次のベスト プラクティスを確認してください。

次に推奨するのは、vSphere HA アドミSSION コントロールのベスト プラクティスです。

- 予約されたクラスタ リソースの割合アドミSSION コントロール ポリシーを選択します。このポリシーは、ホストと仮想マシンのサイズについて最も柔軟です。このポリシーを構成する場合、サポートするホスト障害の回数を反映した CPU とメモリの割合を選択してください。たとえば、vSphere HA で 2 つのホスト障害に対してリソースを取って置いて、クラスタ内に同等のキャパシティのホストが 10 個ある場合には、20% (2/10) と指定します。
- 確実にすべてのクラスタ ホストが同じサイズになるように調節します。クラスタで許容するホスト障害ポリシーについては、クラスタのサイズが異なっていると、vSphere HA で最大のホストのためにキャパシティが予約されるため、障害を処理するために予約されているキャパシティを超過する原因になります。クラスタ リソースの割合ポリシーについては、クラスタのサイズが異なっていると、予期されるホスト障害の回数に対して十分なキャパシティを予約するために、クラスタのサイズが同じ場合よりも多くの割合を指定する必要があります。

- クラスタで許容するホスト障害ポリシーの使用を検討している場合、仮想マシンのサイズ要件が、構成された仮想マシン全体にわたってできるだけ同じになるようにしてください。このポリシーは、スロット サイズを使用して各仮想マシン用に予約する必要があるキャパシティを計算します。スロット サイズは、仮想マシンに必要な最大予約メモリと CPU に基づいています。CPU とメモリ要件の異なる仮想マシンが混在する場合、スロット サイズ計算のデフォルトは可能な最大値になり、統合の制約になります。
- フェイルオーバー ホストの指定ポリシーの使用を検討している場合、何個のホスト障害をサポートするかを決めて、ホストのこの数値をフェイルオーバー ホストとして指定します。クラスタのサイズが異なっている場合、指定されたフェイルオーバー ホストは少なくともクラスタ内の非フェイルオーバー ホストと同じサイズである必要があります。これにより、障害が発生した場合でも十分なキャパシティが確保されます。

## クラスタ監視のベスト プラクティス

vSphere HA クラスタのステータスと有効性を監視するには、次のベスト プラクティスを確認してください。

### アラームの設定によるクラスタ変化の監視

vSphere HA または Fault Tolerance が、仮想マシンのフェイルオーバーなど、可用性維持のためのアクションを実行したときに通知を受けることができます。このようなアクションがトリガーとなるアラームを vCenter Server で設定し、指定した管理者グループにメールなどでアラートを通知できます。

デフォルトで、いくつかの vSphere HA アラームが利用できます。

- フェイルオーバーのリソース不足（クラスタのアラーム）
- プライマリが不明（クラスタのアラーム）
- フェイルオーバー処理中（クラスタのアラーム）
- ホスト HA ステータス（ホストのアラーム）
- 仮想マシン監視エラー（仮想マシンのアラーム）
- 仮想マシン監視アクション（仮想マシンのアラーム）
- フェイルオーバー失敗（仮想マシンのアラーム）

---

**注：** デフォルトのアラームには、vSphere HA の機能名が含まれています。

---

### クラスタの妥当性の監視

有効なクラスタとは、アドミッション コントロール ポリシーに違反していないクラスタです。

vSphere HA が有効に設定されているクラスタが無効になるのは、パワーオンされた仮想マシンの数がフェイルオーバー要件を超えた場合、つまり、現在のフェイルオーバー キャパシティが、構成されたフェイルオーバー キャパシティよりも小さい場合です。アドミッション コントロールが無効な場合は、クラスタが無効になることがあります。

vSphere Web Client で、クラスタの [監視] タブから [vSphere HA] を選択し、[構成の問題] を選択します。vSphere HA の現在の問題が一覧で表示されます。

vSphere HA の問題でクラスタが赤になっても、DRS の動作に影響はありません。

# 仮想マシンの Fault Tolerance の準備

## 3

仮想マシンで vSphere Fault Tolerance を使用して、vSphere HA によって実現されるよりも高いレベルの可用性とデータ保護機能によるビジネス継続性を確保できます。

Fault Tolerance は、ESXi のホスト プラットフォームに構築され、別々のホストで同一の仮想マシンを実行することにより、継続的な可用性を提供します。

フォールトトレランスで最適化の結果を得るには、フォールトトレランスがどのように機能するのか、クラスタおよび仮想マシンに対してフォールトトレランスをどのように有効にするか、および使用法に対するベストプラクティスについてよく理解しておく必要があります。



仮想マシンの Fault Tolerance の保護

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_7ivj3tw/uidConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_7ivj3tw/uidConfId/49694343/))

この章には、次のトピックが含まれています。

- Fault Tolerance の機能
- Fault Tolerance の使用事例
- Fault Tolerance の要件、制限、およびライセンス
- Fault Tolerance の相互運用性
- Fault Tolerance に向けたクラスタとホストの準備
- フォールトトレランスの使用
- Fault Tolerance のベストプラクティス
- レガシー Fault Tolerance

## Fault Tolerance の機能

vSphere Fault Tolerance (FT) は、ほとんどのミッションクリティカルな仮想マシンで使用できます。FT では、継続的に使用できる同一の仮想マシンを別に作成して維持し、フェイルオーバーの発生時にそのマシンで置き換えることにより、ミッションクリティカルな仮想マシンに継続的な可用性を提供します。

保護された仮想マシンは、プライマリ仮想マシンと呼ばれます。複製された仮想マシンであるセカンダリ仮想マシンは、別のホストで作成されて実行されます。セカンダリ仮想マシンは、プライマリ仮想マシンとまったく同じように実行され、いつでも中断されることなく引き継ぐことができます。これにより、フォールトトレランスの保護を実現します。



プライマリ仮想マシンとセカンダリ仮想マシンは、相互にステータスを監視して Fault Tolerance が確保されるようにします。プライマリ仮想マシンが稼動しているホストで障害が発生すると、透過的なフェイルオーバーが行われ、プライマリ仮想マシンの代わりにセカンダリ仮想マシンがすぐにアクティブになります。新しいセカンダリ仮想マシンが起動し、Fault Tolerance の冗長性が自動的に再確立されます。セカンダリ仮想マシンが稼動しているホストで障害が発生すると、その場合もすぐに置き換えられます。いずれの場合も、ユーザーはサービスの中断やデータの損失を意識しません。

フォールトトレランス対応の仮想マシン、およびそのセカンダリコピーは、同じホスト上で実行することはできません。この制限により、ホストで障害が発生しても、仮想マシンが両方とも失われることがなくなります。

---

**注：** また、仮想マシンとホスト間のアフィニティルールを使用して、どのホストで仮想マシンを実行できるかを指定できます。これらのルールを使用する場合は、このようなルールの影響を受けるプライマリ仮想マシンすべてにおいて、関連付けられているセカンダリ仮想マシンも同じルールの影響を受けることを理解しておきます。アフィニティルールの詳細については、ドキュメント『vSphere リソース管理』を参照してください。

---

フォールトトレランスでは、障害からのリカバリ後に1台の仮想マシンの2つのアクティブコピーが存在する、「スプリットブレイン」状態が防止されます。共有ストレージでアトミックファイルロックを使用してフェイルオーバーが調整され、一方のみがプライマリ仮想マシンとして稼動を続け、新しいセカンダリ仮想マシンが自動的に再作成されます。

vSphere Fault Tolerance は、最大で4つのvCPUを持つ対称型マルチプロセッサ(SMP)仮想マシンに対応できます。以前のバージョンのvSphereでは、Fault Tolerance に異なる技術(現在のレガシーFT)が使用されており、要件と特性(レガシーFT仮想マシンでのシングルvCPUの制限を含む)が異なります。それらの以前の要件との互換性が必要な場合は、代わりにレガシーFTを使用できます。ただし、このためには、各仮想マシンについて詳細オプションを設定する必要があります。詳細については[レガシー Fault Tolerance](#)を参照してください。

## Fault Tolerance の使用事例

いくつかの典型的な状況で、vSphere フォールトトレランスを使用してメリットを得ることができます。

フォールトトレランスは、vSphere HA よりも高いレベルのビジネス継続性を実現します。対応するプライマリ仮想マシンを置き換えるためにセカンダリ仮想マシンが呼び出されると、セカンダリ仮想マシンは、仮想マシン全体の状態が保持されまま、すぐにプライマリ仮想マシンのロールを引き継ぎます。アプリケーションはすでに稼動し、メモリに格納されているデータを再入力または再ロードする必要はありません。vSphere HA によるフェイルオーバーでは、障害による影響を受けた仮想マシンが再起動されるという違いがあります。

より高度なレベルの継続性、および状態情報やデータ保護の強化により、フォールトトレランスをデプロイするタイミングのシナリオが通知されます。

- アプリケーションを常に利用できるようにしておく必要がある場合(特に、ユーザーがハードウェアの障害中も維持しておきたい、長期にわたるクライアント接続があるアプリケーション)。
- カスタムアプリケーションで、これよりほかにクラスタリングを行う方法がない場合。
- カスタムクラスタリングソリューションによって高可用性が提供されるが、これらのソリューションが複雑で構成および保持できない場合。



フォールトトレランスを使用して仮想マシンを保護するための、別の重要な使用事例として、オンデマンドのフォールトトレランスを挙げることができます。この場合、通常の操作では、仮想マシンは vSphere HA によって十分に保護されます。特定の重要な期間では、仮想マシンの保護を強化したいことがあります。たとえば、四半期の終わりにレポートを実行することがありますが、このレポートが中断されると、ミッションクリティカルな可用性が妨げられる可能性があります。vSphere Fault Tolerance を使用すると、このレポートを実行する前にこの仮想マシンを保護し、レポートを生成した後で Fault Tolerance をオフまたはサスペンドすることができます。オンデマンドのフォールトトレランスを使用すると、重要な期間に仮想マシンを保護し、重要ではない操作のときには、リソースを通常の状態に戻すことができます。

## Fault Tolerance の要件、制限、およびライセンス

vSphere Fault Tolerance (FT) を使用する前に、この機能に適用される要件、制限、およびライセンスについて検討します。

### 要件

次の CPU 要件とネットワーク要件が FT に適用されます。

フォールトトレランス対応仮想マシンのホストマシンで使用される CPU は、vSphere vMotion と互換性があるか、または Enhanced vMotion Compatibility によって機能強化されている必要があります。また、ハードウェア MMU 仮想化 (Intel EPT または AMD RVI) をサポートする CPU が必要です。次の CPU がサポートされています。

- Intel Sandy Bridge 以降。Avoton はサポートされていません。
- AMD Bulldozer 以降。

FT には 10 Gbit ログ記録ネットワークを使用し、ネットワークが低遅延であることを確認します。FT 専用のネットワークを使用することをお勧めします。

### 制限

Fault Tolerance を使用するように構成されたクラスターでは、2 つの制限が個別に適用されます。

#### **das.maxftvmsperhost**

クラスターの 1 台のホストで許容されるフォールトトレランス対応仮想マシンの最大数。プライマリ仮想マシンとセカンダリ仮想マシンの両方がこの制限に含まれます。デフォルト値は 4 です。

#### **das.maxftvcpusperhost**

ホスト上のすべてのフォールトトレランス対応仮想マシンから集計される vCPU の最大数。プライマリ仮想マシンとセカンダリ仮想マシンの両方の vCPU がこの制限に含まれます。デフォルト値は 8 です。

### ライセンス

1 台のフォールトトレランス対応仮想マシンによってサポートされる vCPU の数は、購入した vSphere のライセンスのレベルによって制限されます。Fault Tolerance は次のようにサポートされます。

- vSphere Standard と vSphere Enterprise。最大 2 つの vCPU を許可

- vSphere Enterprise Plus。最大 4 つの vCPU を許可

**注：** FT とレガシー FT は、vSphere Essentials と vSphere Essentials Plus ではサポートされていません。

## Fault Tolerance の相互運用性

vSphere Fault Tolerance には、vSphere の機能、デバイス、およびその他の相互運用可能な機能に関して、いくつかの制限があります。

vSphere Fault Tolerance を構成する前に、フォールトトレランスと相互運用できない機能および製品について理解しておく必要があります。

### Fault Tolerance でサポートされない vSphere の機能

クラスタを構成するときには、一部の vSphere 機能は Fault Tolerance に組み込むことができないことを理解しておく必要があります。

vSphere の次の機能は、フォールトトレランス対応の仮想マシンに対してサポートされていません。

- スナップショット。仮想マシンで Fault Tolerance を有効にする前に、スナップショットを削除またはコミットしておく必要があります。また、Fault Tolerance が有効になっている仮想マシンでスナップショットを作成することはできません。

**注：** vStorage APIs - Data Protection (VADP) のバックアップで作成されたディスク専用スナップショットは、Fault Tolerance によってサポートされています。ただし、レガシー FT は VADP をサポートしていません。

- Storage vMotion。Fault Tolerance がオンになった仮想マシンに対して、Storage vMotion を起動することはできません。ストレージを移行するには、Fault Tolerance を一時的にオフにして、ストレージの vMotion アクションを実行します。この処理が終了したら、Fault Tolerance をもう一度オンにすることができます。
- リンク クローン。リンク クローンの仮想マシンで Fault Tolerance を使用したり、Fault Tolerance が有効になっている仮想マシンからリンク クローンを作成したりすることはできません。
- 仮想マシン コンポーネント保護 (VMCP)。クラスタで VMCP が有効になっている場合は、この機能がオフになっているフォールトトレランス対応仮想マシンに対してオーバーライドが作成されます。
- 仮想ボリューム データストア。
- ストレージベース ポリシー管理。
- I/O フィルタ。

### Fault Tolerance と互換性のない機能とデバイス

サードパーティのデバイス、機能、または製品の中には、Fault Tolerance と相互運用できないものもあります。

仮想マシンで Fault Tolerance を使用できるようにするには、仮想マシンで次の機能またはデバイスを使用しないでください。

表 3-1. Fault Tolerance と互換性のない機能とデバイス、および対策

互換性のない機能またはデバイス	対策
物理的な Raw ディスク マッピング (RDM)。	レガシー FT により、物理 RDM でバックアップされた仮想デバイスを使用している仮想マシンを、仮想 RDM を使用するように再構成することができます。
物理デバイスまたはリモート デバイスでバックアップされた CD-ROM またはフロッピー仮想デバイス。	CD-ROM またはフロッピー仮想デバイスを削除するか、共有ストレージにインストールされている ISO でバックアップを再構成します。
USB およびサウンド デバイス。	これらのデバイスを仮想マシンから削除します。
N_Port ID Virtualization (NPIV)。	仮想マシンの NPIV 構成を無効にします。
NIC バススルー。	この機能は Fault Tolerance でサポートされていないため、オフにする必要があります。
ホット プラグング デバイス。	<p>フォールトトレランス対応の仮想マシンに対して、ホット プラグ機能は自動的に無効になります。デバイスをホット プラグするには、取り付けの場合でも取り外す場合でも、少しの間 Fault Tolerance をオフにしてホット プラグを実行してから、フォールトトレランスをオンにします。</p> <p><b>注：</b> Fault Tolerance を使用するとき、仮想マシンを実行中に仮想ネットワークカードの設定を変更するのはホット プラグ操作になります。それは、ネットワークカードを「取り外して（アンプラグング）」から再度「取り付け（プラグング）」必要があるからです。たとえば実行中の仮想マシンの仮想ネットワークカード（仮想 NIC）が接続されているネットワークを変更する場合、フォールトトレランスを最初にオフにする必要があります。</p>
シリアルポートまたはパラレルポート	これらのデバイスを仮想マシンから削除します。
3D を有効にしたビデオ デバイス。	Fault Tolerance は、3D を有効にしたビデオ デバイスをサポートしていません。
仮想 EFI ファームウェア	ゲスト OS をインストールする前に、仮想マシンが BIOS ファームウェアを使用するように構成されていることを確認してください。
仮想マシン通信インターフェイス (VMCI)	Fault Tolerance によってサポートされていません。
2TB を超える VMDK	Fault Tolerance は、2TB を超える VMDK ではサポートされていません。

## Fault Tolerance と DRS の併用

vSphere Fault Tolerance は、EVC (Enhanced vMotion Compatibility) 機能が有効になっている場合にのみ、vSphere DRS (Distributed Resource Scheduler) と併用することができます。このプロセスにより、フォールトトレランス対応仮想マシンで、効率的な初期配置の利点を活かすことができます。

クラスターで EVC が有効になっていると、DRS によってフォールトトレランス対応仮想マシンの初期配置が推奨され、DRS の自動化レベルをプライマリ仮想マシンに割り当てることができるようになります（セカンダリ仮想マシンは、対応するプライマリ仮想マシンの設定と常に同じであることを前提とします）。

EVC が無効になっているクラスタ内の仮想マシンで vSphere フォールトトレランスを使用すると、フォールトトレランス対応の仮想マシンの DRS 自動化レベルが「無効」に設定されます。このようなクラスタでは、各プライマリ仮想マシンは登録されているホストでのみパワーオンされ、そのセカンダリ仮想マシンが自動的に配置されます。

フォールトトレランス対応の仮想マシンのペアでアフィニティルールを使用する場合、仮想マシン間のアフィニティルールはプライマリ仮想マシンにのみ適用されますが、仮想マシンとホスト間のアフィニティルールは、プライマリ仮想マシンとそのセカンダリ仮想マシンの両方に適用されます。プライマリ仮想マシンに仮想マシン間のアフィニティルールが設定される場合、DRS は、フェイルオーバー後（つまり、プライマリ仮想マシンが新規ホストに移行した後）に発生した違反を修正しようとします。

## Fault Tolerance に向けたクラスタとホストの準備

クラスタの vSphere Fault Tolerance を有効にするには、機能の前提条件を満たしてから、ホストでいくつかの構成手順を実行する必要があります。これらの手順が完了してクラスタが作成されたあと、構成が Fault Tolerance を有効にするための要件に準拠しているかどうかを確認することもできます。

クラスタの Fault Tolerance を有効にする前に、次のタスクを完了しておく必要があります。

- クラスタ、ホスト、および仮想マシンが、Fault Tolerance チェックリストで概説されている要件を確実に満たすようにする。
- 各ホストのネットワークを構成する。
- vSphere HA クラスタを作成し、ホストを追加して、コンプライアンスをチェックする。

クラスタとホストで Fault Tolerance の準備ができると、仮想マシンのフォールトトレランスをオンにできます。[Fault Tolerance をオン](#) を参照してください。

## Fault Tolerance のチェックリスト

次のチェックリストに記載されているクラスタ、ホスト、仮想マシンの各要件は、vSphere Fault Tolerance を使用する前に認識しておく必要があります。

Fault Tolerance の設定前に、このリストを参照してください。

---

**注：** フォールトトレラント仮想マシンのフェイルオーバーは vCenter Server とは無関係ですが、Fault Tolerance クラスタの設定には vCenter Server を使用する必要があります。

---

## Fault Tolerance でのクラスタ要件

Fault Tolerance を使用する前に、次のクラスタ要件を満たしている必要があります。

- Fault Tolerance のログおよび vMotion ネットワークが構成されている。[ホストマシンのネットワークの構成](#) を参照してください。
- vSphere HA クラスタが作成され、有効です。「[vSphere HA クラスタの作成および構成](#)」を参照してください。フォールトトレランス対応の仮想マシンをパワーオンする前、またはフォールトトレランス対応の仮想マシンがすでにサポートされているクラスタにホストを追加する前に、vSphere HA が有効になっている必要があります。

## Fault Tolerance でのホストの要件

Fault Tolerance を使用するには、次のホストの要件を満たしている必要があります。

- ホストではサポートされるプロセッサを使用する必要があります。
- ホストが Fault Tolerance 用にライセンスされている必要があります。
- ホストが Fault Tolerance 用に認定されている。<http://www.vmware.com/resources/compatibility/search.php> を参照して、[Search by Fault Tolerant Compatible Sets] を選択し、使用するホストが認定されているかどうかを確認します。
- 各ホストの構成で、BIOS のハードウェア仮想化（HV）を有効にしている。

---

**注：** FT 仮想マシンをサポートするために使用するホストでは、BIOS 電源管理設定を「Maximum performance」または「OS-managed performance」に切り替えることをお勧めします。

---

フォールトトレランスをサポートするために、クラスタ内のホストの互換性を確認するには、[クラスタの作成とコンプライアンスのチェック](#)に記載されているように、プロファイルのコンプライアンスチェックを実行することもできます。

## Fault Tolerance での仮想マシンの要件

Fault Tolerance を使用する前に、次の仮想マシンの要件を満たしている必要があります。

- サポートされていないデバイスが仮想マシンに接続されていない。[Fault Tolerance の相互運用性](#)を参照してください。
- フォールトトレランス対応の仮想マシンで、互換性のない機能が実行されていない。[Fault Tolerance の相互運用性](#)を参照してください。
- 仮想マシンファイルが共有ストレージに格納されている。使用できる共有ストレージのソリューションには、ファイバチャネル、（ハードウェアおよびソフトウェア）iSCSI、NFS、および NAS があります。

## 構成に関するその他の推奨事項

Fault Tolerance の構成時には、次のガイドラインにも従ってください。

- 共有ストレージにアクセスするために NFS を使用している場合は、フォールトトレランスが正しく機能するのに必要なネットワークパフォーマンスを得るために、少なくとも 1Gbit NIC の専用 NAS ハードウェアを使用する必要があります。
- Fault Tolerance がオンになると、フォールトトレランス対応仮想マシンのメモリ予約は仮想マシンのメモリサイズに設定されます。必ず、フォールトトレランス対応仮想マシンを含むリソースプールに仮想マシンのメモリサイズより多くのメモリリソースがあるように設定してください。リソースプールに余分なメモリがないと、オーバーヘッドメモリとして使用できるメモリがなくなる場合があります。
- フォールトトレランス対応の仮想マシンごとに、最大 16 個の仮想ディスクを使用します。
- 冗長性を確保し、フォールトトレランスによる最大限の保護を得るためには、クラスタ内に 3 台以上のホストを用意する必要があります。そうすることで、フェイルオーバー時に作成された新しいセカンダリ仮想マシンを収容するホストを確保できます。

## ホスト マシンのネットワークの構成

vSphere HA クラスタに追加する各ホスト上で、2 つの異なるネットワーク スイッチ (vMotion と FT ログ記録) を構成して、ホストが vSphere Fault Tolerance をサポートできるようにする必要があります。

1 台のホストに対して Fault Tolerance を有効にするには、この手順を各ポート グループ オプション (vMotion と FT ログ記録) ごとに実行して、Fault Tolerance のログ記録用に十分なバンド幅を確保する必要があります。一方のオプションを選択し、手順を実行してから、もう一方のポート グループ オプションを選択して再び同じ手順を繰り返します。

### 前提条件

ギガビットのネットワーク インターフェイス カード (NIC) が複数枚必要です。Fault Tolerance をサポートする各ホストについて、最低でも 2 つの物理 NIC を搭載することをお勧めします。たとえば、Fault Tolerance のログ専用に 1 つと、vMotion 専用に 1 つ必要です。可用性を確保するためには、3 つ以上の NIC を使用してください。

---

**注:** vMotion と FT ログ記録 NIC は異なるサブネットに配置する必要があります。レガシー FT を使用する場合、FT ログ記録 NIC では IPv6 はサポートされません。

---

### 手順

- 1 vSphere Web Client で、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[ネットワーク] をクリックします。
- 3 [ホスト ネットワークの追加] アイコンをクリックします。
- 4 接続タイプの選択ページで [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
- 5 [新しい標準スイッチ] を選択して [次へ] をクリックします。
- 6 空いている物理ネットワーク アダプタをスイッチに割り当て、[次へ] をクリックします。
- 7 ネットワーク ラベルを入力し、目的のサービスを有効化して [次へ] をクリックします。
- 8 IP アドレスとサブネット マスクを指定し、設定内容を確認してから [完了] をクリックします。

### 結果

vMotion と Fault Tolerance のログの両方の仮想スイッチを作成したあとに、必要に応じてほかの仮想スイッチを作成できます。ホストをクラスタに追加し、Fault Tolerance をオンにするための手順を完了します。

### 次のステップ

---

**注:** FT をサポートするようネットワークを構成すると、その後 Fault Tolerance のログ用ポートをサスペンドしても、すでにパワーオンされている Fault Tolerance 対応の仮想マシンのペアはパワーオンされたままになります。フェイルオーバーの状況が発生した場合、プライマリ仮想マシンがそのセカンダリ仮想マシンで置き換えられると、新しいセカンダリ仮想マシンは起動されないため、新しいプライマリ仮想マシンは保護されていない状態で動作します。

---

## クラスタの作成とコンプライアンスのチェック

vSphere Fault Tolerance は、vSphere HA クラスタ コンテキストで使用されます。各ホスト上でネットワークを構成したあと、vSphere HA クラスタを作成し、そこにホストを追加します。クラスタが正しく構成されているか、および、クラスタが Fault Tolerance の有効化のための要件に準拠しているかどうかを確認できます。

### 手順

- 1 vSphere Web Client で、クラスタに移動して参照します。
- 2 [監視] タブをクリックし、[プロファイルのコンプライアンス] をクリックします。
- 3 [コンプライアンスを今すぐ確認] をクリックしてコンプライアンス テストを実行します。

### 結果

コンプライアンス テストの結果が表示され、各ホストのコンプライアンスまたはコンプライアンス違反が示されます。

## フォールトトレランスの使用

クラスタ用の vSphere フォールトトレランスを有効にするために必要なすべての手順を行なったあと、個々の仮想マシンでフォールトトレランス機能をオンにすると、この機能を使用できます。

Fault Tolerance をオンにする前に、仮想マシンで検証が実行されます。

これらの検証に合格し、仮想マシンの vSphere Fault Tolerance をオンにすると、そのコンテキストメニューの Fault Tolerance セクションに新しいオプションが追加されます。このオプションには、Fault Tolerance のオフまたは無効化、セカンダリ仮想マシンの移行、フェイルオーバーのテスト、セカンダリ仮想マシンの再起動テストがあります。

## フォールトトレランスをオンにするときの検証

フォールトトレランスをオンにするオプションを利用できる場合であってもこのタスクは検証が必要であり、特定の要件が満たされない場合は失敗する可能性があります。

仮想マシンのフォールトトレランスをオンにするときは、いくつかの検証が行われます。

- vCenter Server 設定で SSL 証明書の確認が有効になっている。
- ホストが vSphere HA クラスタまたは vSphere HA と DRS の混合クラスタに属している。
- ホストに ESXi 6.x 以降（レガシー FT の場合は ESX/ESXi 4.x 以降）がインストールされている。
- 仮想マシンにスナップショットがない。
- 仮想マシンがテンプレートではない。
- 仮想マシンで vSphere HA が無効になっていない。
- 仮想マシンが 3D 対応のビデオ デバイスを持っていない。



## パワーオン状態の仮想マシンの確認

パワーオン済み（またはパワーオン処理中）の仮想マシンに対しては、これ以外の検証も行われます。

- フォールトトレランス機能をオンにする仮想マシンが配置されているホストの BIOS で、ハードウェア仮想化 (HV) が有効になっている。
- プライマリ仮想マシンをサポートするホストのプロセッサがフォールトトレランスに対応している。
- 使用するハードウェアに、フォールトトレランスとの互換性があることが認定されている。互換性があることを確認するには、<http://www.vmware.com/resources/compatibility/search.php> の VMware 互換性ガイドで、[Search by Fault Tolerant Compatible Sets] を選択します。
- 仮想マシンの構成で、フォールトトレランスの併用が有効である。たとえば、サポートしていないデバイスが構成に含まれていない必要があります。

## セカンダリ仮想マシンの配置

仮想マシンのフォールトトレランスをオンにするための検証に合格すると、セカンダリ仮想マシンが作成されます。セカンダリ仮想マシンの配置と初期のステータスは、フォールトトレランスをオンにするときにプライマリ仮想マシンがパワーオンされているか、パワーオフされているかによって異なります。

プライマリ仮想マシンがパワーオンされている場合

- プライマリ仮想マシンの状態がすべてコピーされ、セカンダリ仮想マシンが作成されて、互換性のある別のホストに配置されます。そして、アドミSSION コントロールで許可されるとパワーオンされます。
- 仮想マシンの表示されるフォールトトレランスのステータスは、[保護済み] です。

プライマリ仮想マシンがパワーオフされている場合

- セカンダリ仮想マシンがすぐに作成され、クラスタ内のホストに登録されます（パワーオン時に、より適切なホストに再登録される場合があります）。
- セカンダリ仮想マシンは、プライマリ仮想マシンのパワーオン後にパワーオンされます。
- 仮想マシンの表示されるフォールトトレランスのステータスは、[保護されていません]、[仮想マシンは実行されていません] です。
- フォールトトレランスがオンになったあとでプライマリ仮想マシンをパワーオンしようとする、前述の検証が追加で実行されます。

前述の検証に合格すると、プライマリ仮想マシンとセカンダリ仮想マシンがパワーオンされ、互換性のあるホストに別々に配置されます。仮想マシンのフォールトトレランスのステータスには、[保護済み] というタグが付けられます。

## Fault Tolerance をオン

vSphere Web Client を使用して vSphere Fault Tolerance をオンにすることができます。

Fault Tolerance がオンになると、vCenter Server は仮想マシンのメモリ制限の設定をリセットし、メモリ予約を仮想マシンのメモリサイズに設定します。Fault Tolerance をオンのままにしていると、メモリの予約、サイズ、制限、vCPU 数、シェアを変更できません。また、仮想マシンのディスクを追加または削除することもできません。Fault Tolerance をオフにしても、変更されたパラメータは元の値に戻りません。



クラスタの管理者権限を持つアカウントを使用して、vSphere Web Client を vCenter Server に接続します。

#### 前提条件

次のいずれかの条件に該当する場合、フォールトトレランスをオンにするオプションは利用できません（淡色で表示）。

- この機能がライセンス供与されていないホストに仮想マシンが配置されている。
- メンテナンスモードまたはスタンバイモードのホストに仮想マシンが配置されている。
- 仮想マシンが切断されているか実態なしの状態である（.vmx ファイルにアクセスできない）。
- この機能をオンにする権限がユーザーにない。

#### 手順

- 1 vSphere Web Client で、Fault Tolerance をオンにする仮想マシンに移動して参照します。
- 2 仮想マシンを右クリックし、[Fault Tolerance] - [Fault Tolerance をオンにする] を選択します。
- 3 [可] をクリックします。
- 4 セカンダリ仮想マシンの構成ファイルを配置するデータストアを選択します。その後、[次へ] をクリックします。
- 5 セカンダリ仮想マシンを配置するホストを選択します。その後、[次へ] をクリックします。
- 6 選択内容を確認し、[終了] をクリックします。

#### 結果

指定した仮想マシンはプライマリ仮想マシンとして設定され、セカンダリ仮想マシンがほかのホスト上に作成されます。これで、プライマリ仮想マシンはフォールトトレランス対応になりました。

## Fault Tolerance をオフ

vSphere Fault Tolerance をオフにすると、セカンダリ仮想マシンとその構成、およびすべての履歴が削除されます。

この機能を再び有効にする予定がない場合、[Fault Tolerance をオフにする] オプションを使用します。それ以外の場合は、[Fault Tolerance のサスペンド] オプションを使用します。

---

**注：** セカンダリ仮想マシンが配置されているホストの状態がメンテナンスモード、切断、または応答なしの場合、[Fault Tolerance をオフにする] オプションは使用できません。この場合は、Fault Tolerance をサスペンドして再開する必要があります。

---

#### 手順

- 1 vSphere Web Client で、Fault Tolerance をオフにする仮想マシンに移動して参照します。
- 2 仮想マシンを右クリックし、[Fault Tolerance] - [Fault Tolerance をオフにする] を選択します。
- 3 [はい] をクリックします。

## 結果

選択した仮想マシンで Fault Tolerance がオフになります。選択した仮想マシンの履歴とセカンダリ仮想マシンが削除されます。

## Fault Tolerance のサスペンド

仮想マシンの vSphere Fault Tolerance をサスペンドすると、Fault Tolerance の保護機能はサスペンドされますが、セカンダリ仮想マシンとその構成、およびすべての履歴は維持されます。Fault Tolerance の保護機能を今後再開する場合は、このオプションを使用します。

### 手順

- 1 vSphere Web Client で、Fault Tolerance をサスペンドする仮想マシンを参照します。
- 2 仮想マシンを右クリックし、[Fault Tolerance] - [Fault Tolerance のサスペンド] を選択します。
- 3 [はい] をクリックします。

## 結果

選択した仮想マシンで、Fault Tolerance がサスペンドされます。すべての履歴および選択した仮想マシンのセカンダリ仮想マシンは保存され、今後再開されたときに使用されます。

### 次のステップ

Fault Tolerance をサスペンドした後に、機能を再開する場合は、[Fault Tolerance の再開] を選択します。

## セカンダリの移行

プライマリ仮想マシンの vSphere フォールトトレランスをオンにしたあと、関連付けられたセカンダリ仮想マシンを移行できます。

### 手順

- 1 vSphere Web Client で、セカンダリ仮想マシンを移行するプライマリ仮想マシンに移動して参照します。
- 2 仮想マシンを右クリックし、[Fault Tolerance] - [セカンダリの移行] を選択します。
- 3 [移行] ダイアログボックスでオプション設定を完了し、行った変更を確認します。
- 4 [完了] をクリックして変更内容を適用します。

## 結果

選択したフォールトトレランス機能を持つ仮想マシンに関連付けられているセカンダリ仮想マシンが、指定したホストに移行されます。

## フェイルオーバーのテスト

選択したプライマリ仮想マシンにフェイルオーバーの状況を発生させ、Fault Tolerance による保護をテストできます。

仮想マシンがパワーオフ状態の場合、このオプションは利用できません（灰色で表示）。

#### 手順

- 1 vSphere Web Client で、フェイルオーバーをテストするプライマリ仮想マシンに移動して参照します。
- 2 仮想マシンを右クリックし、[Fault Tolerance] - [フェイルオーバーのテスト] を選択します。
- 3 タスク コンソールにフェイルオーバーに関する詳細が表示されます。

#### 結果

このタスクでは、プライマリ仮想マシンに障害を発生させて、セカンダリ仮想マシンへのフェイルオーバーが行われることを確認します。新規のセカンダリ仮想マシンも起動し、プライマリ仮想マシンが保護済みの状態に戻ります。

## セカンダリの再起動テスト

セカンダリ仮想マシンに障害を発生させて、選択したプライマリ仮想マシンで提供される Fault Tolerance の保護をテストできます。

仮想マシンがパワーオフ状態の場合、このオプションは利用できません（灰色で表示）。

#### 手順

- 1 vSphere Web Client で、テストを実行するプライマリ仮想マシンに移動して参照します。
- 2 仮想マシンを右クリックし、[Fault Tolerance] - [セカンダリの再起動テスト] を選択します。
- 3 タスク コンソールにテストに関する詳細が表示されます。

#### 結果

このタスクによって、選択したプライマリ仮想マシンに Fault Tolerance の保護を提供するセカンダリ仮想マシンが停止します。新規のセカンダリ仮想マシンが起動し、プライマリ仮想マシンが保護済みの状態に戻ります。

## Fault Tolerance で使用するホストのアップグレード

次の手順を使用して、Fault Tolerance に使用するホストをアップグレードします。

#### 前提条件

クラスタの管理者権限があることを確認します。

パワーオンされたフォールトトレランス対応の仮想マシンをホストする、4 台以上の ESXi ホストのセットがあることを確認します。仮想マシンがパワーオフされている場合は、プライマリとセカンダリの仮想マシンを異なるビルドのホストに再配置できます。

---

**注：** このアップグレード手順は、最低 4 ノードのクラスタ用のものです。さらに小規模なクラスタでも同じ手順で実行できますが、保護されない期間が多少長くなります。

---

#### 手順

- 1 vMotion を使用して、2 台のホストからフォールトトレランス対応の仮想マシンを移行します。
- 2 退避した 2 台のホストを同じ ESXi ビルドにアップグレードします。
- 3 プライマリ仮想マシンで Fault Tolerance をサスペンドします。

- 4 VMotion を使用して、Fault Tolerance をサスペンドしたプライマリ仮想マシンを、アップグレードされたホストの 1 つに移動します。
- 5 移動したプライマリ仮想マシンで Fault Tolerance を再開します。
- 6 アップグレード後のホストに格納可能なフォールトトレランス対応仮想マシンペアの数だけ、[手順 1](#) から [手順 5](#) を繰り返します。
- 7 vMotion を使用して、フォールトトレランス対応の仮想マシンを再配分します。

## 結果

クラスタ内のすべての ESXi ホストがアップグレードされます。

# Fault Tolerance のベスト プラクティス

Fault Tolerance の結果を最適化するには、特定のベスト プラクティスに従う必要があります。

ホストとネットワーク構成に関する以下の推奨事項を実行することで、クラスタの安定性とパフォーマンスを高めることができます。

## ホスト設定

プライマリ仮想マシンとセカンダリ仮想マシンを実行しているホストは、ほぼ同じプロセッサ周波数で動作している必要があります。周波数が大きく異なると、セカンダリ仮想マシンが頻繁に再起動する場合があります。ワークロードに基づいて調整されないプラットフォームでは、電源管理機能（電力を節約するためのパワー キャッピングや強制的な低周波数モードなど）によって、プロセッサの周波数が大きく異なる可能性があります。セカンダリ仮想マシンが定期的に再起動する場合は、Fault Tolerance 対応の仮想マシンを実行するホストですべての電源管理モードを無効にするか、すべてのホストが同じ電源管理モードで動作するようにします。

## ホスト ネットワーク構成

次のガイドラインで説明するように、トラフィック タイプ（たとえば NFS）と複数の物理 NIC をさまざまに組み合わせ、Fault Tolerance をサポートするホストのネットワークを構成できます。

- 各 NIC チームを 2 台の物理スイッチ経由で配布して、2 台の物理スイッチ間の各 VLAN の L2 ドメインの継続性を確保する。
- 明確なチームング ポリシーを使用して、特定のトラフィック タイプが、特定の NIC（アクティブ/スタンバイ）または NIC のセット（たとえば送信元仮想ポート ID）に対してアフィニティを持つようにする。
- アクティブ/スタンバイ ポリシーを使用する場合は、2 つのトラフィック タイプを実装して、両方のトラフィック タイプが 1 枚の vmnic を共有することで、フェイルオーバーする前の影響を最小にする。

- アクティブ/スタンバイ ポリシーを使用する場合は、特定のトラフィック タイプ（たとえば FT ログ記録）用のすべての有効なアダプタを、同一の物理スイッチに構成する。これにより、ネットワークのホップ数を最小限にし、スイッチ間のリンクが超過する可能性を減らすことができます。

**注：** プライマリ仮想マシンとセカンダリ仮想マシン間の FT ログ記録トラフィックは暗号化されず、ゲスト ネットワークおよびストレージ I/O データと、ゲスト OS のメモリの内容が含まれます。このトラフィックには、パスワードなどの機密情報がプレーンテキストで含まれる可能性があります。このようなデータの漏洩を回避するため、このネットワークは確実にセキュリティ保護し、特に中間者攻撃が防止されるように注意してください。たとえば、FT ログ記録トラフィック用にプライベート ネットワークを使用できます。

## 同種のクラスタ

vSphere Fault Tolerance は、異種ホストが含まれているクラスタでも機能しますが、互換性のあるノードを持つクラスタで最高の性能を発揮します。クラスタを構築するとき、すべてのホストが次の構成になっている必要があります。

- 仮想マシンで使用するデータストアへの共通アクセス。
- 同じ仮想マシンのネットワーク構成。
- すべてのホストで同じ BIOS 設定（電源管理とハイパースレッディング）。

[コンプライアンスの確認] を実行して互換性のないものを特定し、修正します。

## パフォーマンス

プライマリ仮想マシンとセカンダリ仮想マシン間のトラフィックをログするために使用できるバンド幅を増やすには、10Gbit NIC を使用し、ジャンボ フレームの使用を有効にします。

## 共有ストレージ上の ISO による継続アクセス

Fault Tolerance が有効な仮想マシンがアクセスする ISO は、フォールト トレランス対応の仮想マシンの両方のインスタンスがアクセス可能な共有ストレージに格納します。この構成では、仮想マシンの CD-ROM はフェイルオーバーが発生しても正常に動作します。

Fault Tolerance が有効な仮想マシンでは、プライマリ仮想マシンのみアクセス可能な ISO イメージを使用することもできます。このような場合、プライマリ仮想マシンは ISO にアクセスできますが、フェイルオーバーが生じると、CD-ROM はメディアがないことを示すエラーを報告します。パッチの適用などの一時的で重要性が低い操作に CD-ROM を使用する場合は、この状況でもほとんど問題はありません。

## ネットワーク パーティション分割の回避

ネットワーク パーティション分割が発生するのは、vSphere HA クラスタの管理ネットワークに障害が起こり、ホストの一部が vCenter Server や他のホストから分離されたときです。[ネットワーク パーティション](#) を参照してください。パーティション分割が発生すると、Fault Tolerance による保護が脆弱になる場合があります。

Fault Tolerance を使用する vSphere HA クラスタがパーティション分割されると、プライマリ仮想マシン（またはそのセカンダリ仮想マシン）に対する責任のないプライマリ ホストによって管理されるパーティションに、これらの仮想マシンが配置される可能性があります。フェイルオーバーが必要な場合に、セカンダリ仮想マシンが再起動されるのは、プライマリ仮想マシンに責任のあるプライマリ ホストによって管理されるパーティションに、プライマリ仮想マシンが配置されている場合のみです。

管理ネットワークにネットワーク パーティション分割が生じるような障害が発生しないように、[ネットワークのベスト プラクティス](#)の推奨を実行してください

## Virtual SAN データストアの使用

vSphere Fault Tolerance は Virtual SAN データストアを使用できますが、次の制限に注意する必要があります。

- Virtual SAN と他のタイプのデータストアの混在は、プライマリ仮想マシンでもセカンダリ仮想マシンでもサポートされません。
- Virtual SAN の Metro クラスタは FT ではサポートされません。

FT を Virtual SAN と併用した環境でパフォーマンスと信頼性を向上させるには、次の構成が推奨されます。

- Virtual SAN と FT に個別のネットワークを使用する。
- プライマリ仮想マシンとセカンダリ仮想マシンを、個別の Virtual SAN フォールト ドメインに配置する。

## レガシー Fault Tolerance

デフォルトでは、vSphere Fault Tolerance (FT) は、最大で 4 つの vCPU を持つ対称型マルチプロセッサ (SMP) 仮想マシンに対応できます。ただし、仮想マシンの vCPU が 1 つだけの場合は、下位互換性を保つため、代わりにレガシー FT を使用できます。技術的に必要な場合以外は、レガシー FT の使用はお勧めしません。

レガシー Fault Tolerance を使用するには、仮想マシンの詳細オプションを構成する必要があります。この構成を完了した後のレガシー FT 仮想マシンは、いくつかの点で他のフォールト トレランス対応仮想マシンと異なっています。

## レガシー FT を使用する仮想マシンの相違点

FT を使用する仮想マシンとレガシー FT を使用する仮想マシンは、いくつかの点で異なります。

表 3-2. レガシー FT と FT の相違点

	レガシー FT	FT
Extended Page Tables/Rapid Virtualization Indexing (EPT/RVI)	サポート対象外	必須
IPv6	レガシー FT ログ記録 NIC ではサポート対象外。	FT ログ記録 NIC ではサポート対象。
DRS	初期配置、ロード バランシングが完全にサポート対象で、メンテナンス モードもサポートされます。	セカンダリ仮想マシンのパワーオン配置とメンテナンス モードのみがサポート対象です。
vStorage API - データ保護バックアップ	サポート対象外	サポート対象

表 3-2. レガシー FT と FT の相違点（続き）

	レガシー FT	FT
Eager-zeroed シック .vmdk ディスク ファイル	必須	FT がシックとシンを含むすべてのディスク ファイル タイプをサポートするため不要です
.vmdk の冗長性	1 つのコピーのみ	プライマリ仮想マシンとセカンダリ仮想マシンが常に独立したコピーを保持します。冗長性を高めるため、別々のデータストアに配置できます。
NIC 帯域幅	専用の 1GB NIC を推奨	専用の 10GB NIC を推奨
CPU およびホストの互換性	各ホストに、同一の CPU モデルとファミリー、およびほぼ同じバージョンの vSphere が必要です。	CPU は、vSphere vMotion または EVC と互換性がある必要があります。ホスト上の vSphere のバージョンは、vSphere vMotion と互換性がある必要があります。
実行中の仮想マシンでの FT の有効化	常にサポートされるとは限りません。まず仮想マシンをパワーオフする必要がある場合があります。	サポート対象
Storage vMotion	パワーオフされた仮想マシンでのみサポートされます。  vCenter Server は、Storage vMotion のアクションを実行する前に自動的に FT をオフにし、Storage vMotion のアクションが完了してから FT を再び有効にします。	サポート対象外。ユーザーは、まずその仮想マシンの FT を無効にしてから、Storage vMotion のアクションを実行し、再び FT を有効にする必要があります。
vlsance ネットワーク ドライバ	サポート対象外	サポート対象

## レガシー FT のその他の要件

レガシー FT には、一覧にある相違点に加えて、次のような特有の要件もあります。

- クラスタには、同じバージョン番号の Fault Tolerance または同じホストのビルド番号が実行されている FT 認定ホストが、少なくとも 2 つ含まれている必要があります。Fault Tolerance のバージョン番号は、vSphere Web Client のホストの [サマリ] タブに表示されます。
- 各 ESXi ホストは、同じ仮想マシンのデータストアおよびネットワークにアクセスできる必要があります。
- 仮想マシンが、仮想 RDM またはシック プロビジョニングされた仮想マシン ディスク（VMDK）ファイルに格納されている必要があります。仮想マシンがシン プロビジョニングされた VMDK ファイルに格納されている場合に Fault Tolerance を使用しようとする、VMDK ファイルを変換する必要があることを示すメッセージが表示されます。変換を行うには、仮想マシンをパワーオフする必要があります。
- ホストは、FT 対応のプロセッサ グループのプロセッサを装備している。ホストのプロセッサ間で、相互に互換性があることを確認してください。
- セカンダリ仮想マシンをサポートするホストのプロセッサがフォールトトレランスに対応し、またプライマリ仮想マシンをサポートするホストと同じ CPU ファミリまたはモデルである。

- フォールト トレランス対応仮想マシンが存在するホストをアップグレードする際は、プライマリ仮想マシンとセカンダリ仮想マシンが、FT のバージョン番号またはホストのビルド番号 (ESX/ESXi 4.1 以前のホストの場合) が同じホストで動作し続けることを確認してください。

---

**注：** クラスタ内のホストをアップグレードする前に、レガシー FT を使用するように仮想マシンを指定した場合、その仮想マシンは、ホストのアップグレード後も引き続きレガシー FT を使用します。

---

## レガシー Fault Tolerance の有効化

レガシー Fault Tolerance を使用するには、仮想マシンの詳細オプションを構成する必要があります。

レガシー FT は、まだ FT を使用していないシングル vCPU の仮想マシンでのみ使用することができます。レガシー FT を使用する各仮想マシンでレガシー FT を有効にするには、`vm.uselegacyft` の詳細オプションの値を `[true]` にする必要があります。

### 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 仮想マシンを右クリックし、**[[設定の編集]]** を選択します。
- 3 **[仮想マシン オプション]** タブをクリックします。
- 4 **[詳細]** セクションを開き、**[構成パラメータ]** の横で **[構成の編集]** をクリックします。
- 5 **[行の追加]** をクリックし、**[名前]** に `vm.uselegacyft` と入力し、**[値]** に `[true]` と入力します。
- 6 **[[OK]]** をクリックします。

### 結果

これで、その仮想マシンでレガシー FT が有効になります。